INSTITUTO SUPERIOR
DE TECNOLOGIAS
AVANÇADAS DE LISBOA

Proteção de Dados na Computação em Nuvem

Inocêncio Neto Barros

Dissertação para obtenção do Grau de Mestre em

INFORMÁTICA

Presidente: Professor Doutor Paulo André Reis Duarte Branco

Arguente: Professor Doutor Paulo Jorge Gonçalves Pinto

Orientador: Professora Doutora Isabel Maria Surdinho Borges Alvarez

Março, 2021

Índice

Índice de Figuras e Tabelas

Dedicatória

Dedico este trabalho aos meus colegas, amigos, familiares e ao Professor Nuno Mingato.

Agradecimentos

Agradeço ao Ayrton Jorge e o Arlécio Pequeno, pela força ao longo desta caminhada, aos professores pelo método implementado, para nos obrigar a estarmos preparados para esta fase da dissertação que é a mais exigente, à minha orientadora pelo apoio ao longo deste percurso exigente e, em simultâneo, interessante, não esquecendo a minha namorada, amigos e familiares que sempre me deram um apoio incondicional.

Abreviaturas

AWS — Amazon Web Service

CCPA — California Consumer Privacy Act

CDPA — Consumer Data Privacy Act

CGPD — Comité Gestor de Proteção de Dados

CPRA — California Privacy Rights Act

CSP — Cloud Service Provider

DPD — Data Protection Directive

DPIA — Data Protection Impact Assessment

DPO — Data Protection Officer

ECPA — Electronic Communications Privacy Act

EEE — Espaço Económico Europeu

EUA — Estados Unidos de América

FCRA — Fair Credit Reporting Act

FTC — Federal Trade Commission

HHS — Health and Human Services

IaaS — Infrastructure as a Service

IBM — International Business Machines

IP — Internet Protocol

LGPD — Lei Geral de Proteção de Dados

OCDE — Organização para a Cooperação e Desenvolvimento Económicos

NIST — National Institute of Standard Technology

NYPA — New York Privacy Act

PaaS — Platform as a Service

PDA — Personal Data Analyzer

RGPD — Regulamento Geral de Proteção de Dados

SaaS — Software as a Service

TI — Tecnologia de Informação

UE — União Europeia

WPA — Washington Privacy Act

W3C — World Wide Web Consortium

Resumo

Nos últimos anos, a computação em nuvem tem evoluído muito, mas, em simultâneo, aumentaram as ameaças, isto por os dados serem acedidos pela Internet. Como a maioria dos centros de dados estão fora da União Europeia (UE) e se encontram localizados nos Estados Unidos da América (EUA), o investigador fez um estudo exaustivo sobre as leis de proteção de dados que se aplicam nos dois espaços geográficos. O objeto deste estudo baseia-se na recolha de informações necessárias e comparação sobre a forma como os dados pessoais são tratados na União Europeia e nos Estados Unidos da América.

Na UE, abordou-se o Regulamento Geral de Proteção de Dados, como ponto de partida na recolha de informações sobre os direitos dos titulares dos dados, Princípios Básicos de Processamento, Processamento de Dados Pessoais, Princípio de Privacidade para Proteção de Dados, Requisitos Organizacionais e, a seguir, Justificação Legal para o Tratamento de Dados. Enquanto, nos EUA, por ter uma abordagem completamente diferente da UE, começou-se por referir um pouco a história por detrás e, a seguir, abordaram-se as Leis de Privacidade do Consumidor de Califórnia, representado por CCPA, Lei de Proteção de Dados dos Consumidores da Virgínia representado por CDPA, de forma aprofundada, Leis de Privacidade de Washington, representado por WPA, e Leis de Privacidade de Nova Iorque, representado por NYPA, de uma forma superficial. O estudo foca-se na forma de recolha, processamento, transferência, violação e prevenção de acesso de pessoas não autorizadas; foi seguidamente feita uma comparação direta entre RGPD e CCPA, onde se abordam os direitos dos titulares dos dados, quem é protegido, a informação protegida e regulada pelas entidades.

Após se ter efetuado a comparação entre o RGPD e o CCPA, fez-se também uma interligação entre os resultados da comparação anterior com a computação em nuvem, com novas responsabilidades para os CSPs enquanto Processador, Clientes ou Fornecedor como Controlador, Políticas de Armazenamento e Processamento, Consentimento dos Titulares de Dados para os Serviços na Nuvem, Segurança e Violação, Localização, Transferência e Eliminação dos Dados.

Palavras-chave: Computação em Nuvem, Privacidade de Dados, RGPD, CCPA, CDPA

Abstract

In recent years, cloud computing has evolved a lot, but at the same time, threats have increased because data is accessed over the Internet. As most data centers are outside the European Union (EU) and are located mainly in the United States of America (USA), the researcher thoroughly studied the data protection laws that apply in both geographic spaces. The subject of this study is based on the collection of necessary information and comparison of how personal data is handled in the European Union and the United States of America (USA).

In the EU, the study focused on the GDPR deepening the collection of information on the rights of data subjects, Basic Principles of Processing, Processing of Personal Data, Principle of Privacy for Data Protection, Organizational Requirements and then Legal Justification for Data Processing, while in the USA, by having a completely different approach that in the EU we started by talking a little about the history behind and then, addressed on the CCPA and CDPA in-depth and WPA and NYPA superficially. First, the study focuses on the form of collection, processing, transfer, violation, and prevention of access of unauthorized persons. Then, a direct comparison was made between GDPR and CCPA, which addresses the rights of data subjects, which are protected, the information protected and regulated by the entities.

After comparing GDPR and CCPA, there was also a link between the results of the previous comparison with cloud computing, where they bring new responsibilities to CSPs as Processor, Customers or Supplier as Controller, Storage and Processing Policies, Consent of Data Subject to Cloud Services, Data Security, Violation, Location, Transfer and Erasing.

Key Words: Cloud Computing, Data Privacy, GDPR, CCPA, CDPA

1 Introdução

1.1 Enquadramento e Motivação

Atualmente, a computação em nuvem é considerada o paradigma de computação mais recente que oferece numerosos serviços consistentes e flexíveis usando tecnologia de virtualização que é usado na próxima geração dos *datacenters*. Não só empresas privadas e particulares, mas também departamentos do governo estão a aumentar o serviço de disponibilidade através da infraestrutura de computação em nuvem. Através da sua capacidade, resiliência e minimização de custos que fornece a capacidade de compartilhar recursos de forma abrangente e transparente, a computação em nuvem também tem a capacidade de realizar procedimentos que vão ao encontro de diferentes necessidades (Issi & Ef, 2018).

A nuvem está a revolucionar os nossos ecossistemas com métodos de processamento e benefícios significativos, tais como a disponibilidade de ferramentas automatizadas para montar, ligar, configurar e reconfigurar recursos virtualizados a pedido; com isso, torna muito mais fácil cumprir os objetivos organizacionais, dado que as organizações podem facilmente implementar serviços na nuvem (Laure, 2016).

Com o desenvolvimento tecnológico, houve um aumento significativo nos requisitos de privacidade e proteção de dados com intuito de proteger os dados dos indivíduos. Entretanto, a legislação de proteção como antiga Diretiva de Proteção de Dados da UE (DPD), atual RGPD e a Lei de Portabilidade e Responsabilização dos Seguros de Saúde dos EUA (HIPAA), entre outras entidades nos EUA, exigem a preservação da privacidade para o tratamento de informações pessoalmente identificáveis (Laure, 2016).

Hoje, a maior parte das transações acontecem online. As entidades que gerem essas aplicações terão que estar em conformidade com a nova legislação, que protege os dados dos cidadãos europeus dentro ou fora da União Europeia (Peasley, 2019).

A forma como expomos os nossos dados pessoais na Internet, seja nas redes sociais ou em qualquer outro sítio web onde efetuamos as nossas transações, requer algum cuidado, isto porque não sabemos onde os dados estão armazenados e o que a pessoa do outro lado pode fazer com esses dados.

Um dos motivos que fez com que o investigador aprofundasse este tema, é, principalmente, para estar por dentro dos direitos e da segurança associada aos seus dados pessoais quando exposto num sítio web, sendo ele dentro ou fora da UE, e também dar a conhecer aos leitores uma visão geral sobre o papel das entidades que protegem os direitos dos titulares dos dados.

Tendo em conta as leis sob a alçada do RGPD, entidade que controla como os dados pessoais são processados de todos os cidadãos que residem dentro ou fora da UE (Bussche, 2017), os utilizadores podem sentir-se mais seguros quando criam um perfil com os dados verdadeiros nos sítios web, seja para efetuar uma transação ou por outro motivo. Dado que a empresa que gere o *site* tem que providenciar privacidade e segurança dos dados pessoais que ali se encontram. O mesmo se aplica aos EUA, visto que ali seguem os mesmos passos da União Europeia.

Antes do RGPD, existia uma entidade que se chamava Europeia de Proteção de Dados, fazia o mesmo trabalho, mas o RGPD trouxe maior controlo e atribuição de responsabilidades perante pessoas singulares ou coletivas (Stendal, 2020). Os EUA seguiram o mesmo passo da UE, mas ligeiramente diferente no que toca à privacidade dos dados aplicados a pessoas singulares ou coletivas (Ventura, 2020). Nos EUA, cada estado tem a sua própria entidade para regular a privacidade dos dados dos cidadãos norte-americanos. Segundo Luca Ventura (2020), o estado da Califórnia foi dos primeiros a aprovar o regulamento, e segue as mesmas leis que o RGPD na matéria de direitos e proteção de Dados de Cidadãos californianos.

Para os fornecedores da nuvem estarem em conformidade com as entidades que regulam a privacidade de pessoas singulares ou coletivas, foi necessário introduzir novas funções que são o Processador de Dados e o Controlador de dados. Segundo Barbara Russo (2018), o fornecedor de serviço pode desempenhar as duas funções: se um fornecedor é um processador de dados, um cliente de serviços em nuvem é geralmente considerado um controlador dos dados armazenados nos servidores do fornecedor.

1.2 Metodologia de Investigação

O foco principal desta dissertação está nas preocupações levantadas acerca da privacidade dos dados nas instituições que utilizam a computação em nuvem, o que requer uma investigação bastante rigorosa acerca da privacidade dos dados dos clientes das empresas em geral. No entanto, ao utilizar dados na nuvem, tem que se ter em conta as considerações éticas e regulamentares relacionadas com a propriedade dos dados. Esses dados devem ser tratados de forma transparente, para que as identidades dos indivíduos que possuem os dados não sejam reveladas. As soluções em nuvem devem proteger a privacidade dos dados dos clientes de forma adequada. No entanto, a legislação existente impede as instituições de processar, usar a nuvem em partes devido à forma como as funções de gestão de dados são definidos no presente e, também, devido às restrições impostas pelas regras em vigor.

Inicialmente, foi feita uma revisão sistemática da literatura (Okoli, 2015) para identificar, selecionar e investigar os artigos mais relevantes relacionados com os temas desta investigação para descrição e explicação da situação em estudo. Posteriormente, foi realizado um estudo comparativo (Fachin, 2001), para explicar as semelhanças e diferenças, entre os dados pesquisados sobre a situação encontrada na UE e nos EUA, deduzindo as suas semelhanças e diferenças, aplicadas à computação em nuvem.

1.2.1 Questões e Contributos de Investigação

Os principais contributos desta dissertação estão alinhados nas três principais questões de investigação, introduzidas e discutidas abaixo:

- **P1**: Quem controla o modo como os dados pessoais são tratados por uma empresa na Europa?

- **P2**: O que as entidades estatais e empresas devem fazer, para garantir a privacidade dos Dados nos Estados Unidos de América?

- **P3**: Como é feita a integração entre privacidade de Dados na Europa e nos Estados Unidos de América?

- **C1**: O primeiro contributo desta dissertação, consiste em dar a conhecer aos leitores um entendimento sobre a privacidade dos dados, e de como os dados podem ser processados pelo Regulamento Geral sobre a Proteção de Dados. Esta entidade foi implementada, com o intuito de controlar a forma como os dados dos cidadãos europeus podem ser processados. Este regulamento abrange também cidadãos europeus fora da zona europeia. As informações mais detalhadas sobre o RGPD estarão presentes no capítulo III desta dissertação, a fim de especificar as características relevantes de uma metodologia de modelação e de ameaças à privacidade dos dados no seu todo.

- **C2**: O modo como se aplica a privacidade dos dados nos Estados Unidos da América é completamente diferente da União Europeia, isto porque nos EUA, cada estado tem a sua própria entidade para lidar com questões referentes a privacidade e segurança de dados. Os mais conhecidos são: o *California Consumer Privacy Act (CCPA)* em *2018* e *California Privacy Rights Act (CPRA) em 2020 e Virginia Consumer Data Privacy Act (CDPA),* mas existem muitos outros. Cada entidade tem a sua forma de processar e proteger os dados dos cidadãos/ clientes, com definições extensivas de informações pessoais, concedendo aos clientes/ consumidores/ cidadãos, direitos sobre as suas informações pessoais e exigindo que as empresas cobertas facultem um aviso transparente acerca das suas práticas.

- Embora existam muitas semelhanças entre estas leis, também existem algumas diferenças importantes. Informações detalhadas sobre este tema estão presentes no capítulo quatro desta dissertação, onde se abordará de forma detalhada a privacidade de dados nos EUA.

- **C3**: Neste contributo introduzimos, finalmente, a metodologia comparativa, com que iremos comparar a forma como se aplica a privacidade dos dados nos

EUA e na Europa. O RGPD é aplicável aos dados pessoais dos titulares dos dados, enquanto o CCPA é aplicável especialmente aos consumidores e famílias. Foi feito um apanhado de informações acerca da privacidade dos dados na UE, nos EUA e as respetivas entidades responsáveis e, por último, interligou-se a computação em nuvem com a privacidade dos dados, para garantir conformidade, com as entidades que regulam o processamento dos dados pessoais nas duas regiões.

1.2.2 Método de Pesquisa

Estas são as etapas que foram levadas a cabo na pesquisa descrita nesta dissertação:

- Na primeira etapa da investigação, foi realizado um estudo exaustivo e preliminar da literatura apropriada que abrangeu os tópicos relevantes, como a computação em nuvem, as entidades que controlam e protegem dados pessoais, consumidores e famílias tanto nas empresas como na nuvem;

- Na segunda etapa da investigação, fez-se uma comparação na forma como os dados pessoais e sensíveis são tratados na União Europeia e nos Estados Unidos da América, no geral, tendo como objeto da comparação: a Restrição à Recolha de Dados e a Garantia de Dados Corretos, Restrição no Processamento/ Tratamento de Dados, Restrição à Transferência de Dados, Violação e Prevenção de Acessos Não Autorizados; a seguir fez-se uma comparação direta entre o RGPD — UE e o CCPA — EUA tendo como objeto da comparação: a Portabilidade dos Dados, Eliminação, Retificação, Restringir o Processamento, Quem é regulado, Quem está protegido, Que informação é protegida.

- Na terceira e última etapa de investigação, interligaram-se os resultados do estudo comparativo entre a situação na EU e os EUA com a Computação na Nuvem, onde se centrou nas novas funções dos Fornecedores de Serviços em Nuvem como Processador ou Controlador, nas Políticas de Armazenamento e Processamento, Segurança e Violação, Localização, Transparência, Eliminação e Consentimento dos Titulares dos Dados para Serviços na Nuvem. O objetivo, consistiu em validar se os Fornecedores dos Serviços da Nuvem estão em conformidade com as leis publicadas; a seguir focou-se nas

características de Computação na Nuvem, e efetuou-se a comparação com os artigos de RGPD.

1.3 Estrutura da Dissertação

O capítulo dois contém um estudo aprofundado sobre a computação em nuvem, no qual se abordaram temas tais como a definição proveniente de diferentes investigadores, tipos de serviços, modelos de implementação e benefícios em aderir, sem esquecer as suas características essenciais.

O Capítulo três tem uma revisão exaustiva sobre o RGPD, contemplando desde eventos que fizeram com que fosse aprovada pela Comissão Europeia até agora. Sobre o RGPD focou-se apenas a parte tecnológica, na qual se lida com dados sensíveis e pessoais, ou seja, por outras palavras, neste capítulo, abordam-se as inúmeras definições existentes, um pouco sobre a história por detrás assim com a entidade antes de RGPD que se denominava “Diretiva da Proteção de Dados Pessoais”. A seguir, manteve-se o foco na parte de Segurança e Processamento de Dados Pessoais, Princípios de Privacidade para a Proteção de Dados, Direitos do Titular dos Dados e Princípios de Legalidade do Processamento, e as coimas associadas para as empresas que violarem as leis impostas, de forma detalhada.

O Capítulo quatro contém uma descrição completa sobre a forma como se gerem os dados pessoais dos titulares/ consumidores/ clientes nos Estados Unidos de América, começando por abordar um pouco sobre a história da privacidade nos EUA.

Neste capítulo, começa-se com uma abordagem geral sobre a privacidade no seu todo, de seguida, aborda-se a história que começa em 1890, que é quando surgiu o primeiro artigo sobre o direito à privacidade.

No capítulo cinco, realizou-se uma comparação entre a UE e os EUA no que toca à privacidade dos dados, começando pelas restrições e recolha dos dados, restrições no processamento dos dados, restrições à transferência dos dados, violação e prevenção de acesso não autorizado, e entramos no campo onde se compara CCPA com RGPD, concluindo-se com um quadro que se centra nos direitos dos titulares dos dados, pessoas abrangidas e informação protegidas.

No capítulo seis, fez-se uma interligação entre a privacidade de dados e computação em nuvem.

2 Computação em Nuvem

2.1 Definição

O NIST definiu computação em nuvem como um modelo, para permitir o acesso ubíquo e conveniente à rede a pedido de um conjunto partilhado de recursos de computação configuráveis (redes, servidores, armazenamento, serviços e aplicações) que pode ser rapidamente aprovisionado e libertado, com o mínimo esforço de gestão ou interação do prestador de serviços (Simmon, 2018).

Computação em nuvem, significa desenvolvimento e aplicação de tecnologia de computação baseada na Internet. Este termo é um método de cálculos informáticos, num espaço em que as capacidades baseadas em TI são apresentadas como um serviço para o utilizador, podendo ter acesso a serviços baseados em tecnologia na Internet, sem informação especializada sobre estas tecnologias ou ter o controlo de infraestruturas tecnológicas que as suportam. Trata-se assim de um conceito geral, que está a ser usado para a integração de novas tecnologias, incluindo *software* como serviço, *web* e outras novas soluções apresentadas recentemente, podendo atender a todos os requisitos do utilizador no espaço Internet. A computação em nuvem, é um modelo para permitir o acesso conveniente e a pedido da rede, a um conjunto partilhado de recursos de computação configuráveis, que podem ser rapidamente aprovisionados e libertados com o mínimo esforço de gestão ou interação do prestador de serviços (Taghipour, Mowloodi, Mahboobi, & Abdi, 2020) Taghipou.

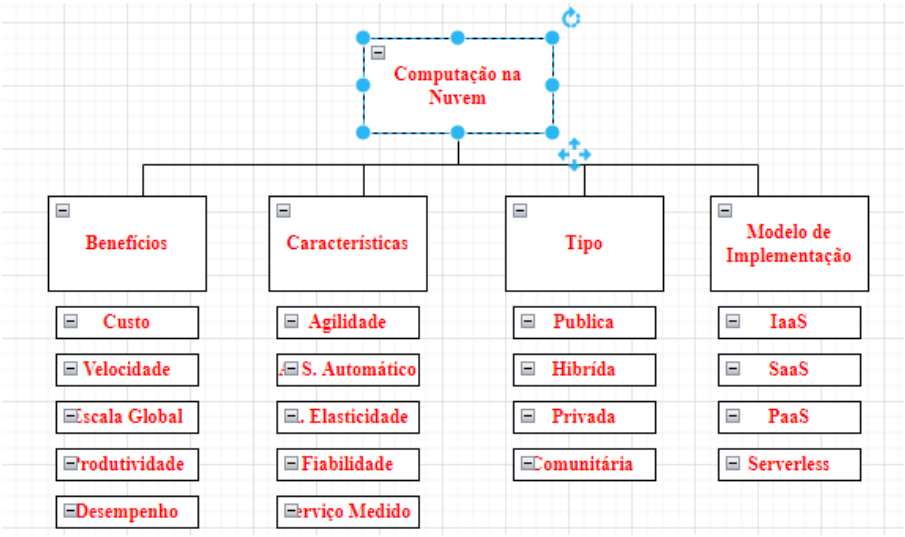

Figura 1 Computação em Nuvem — Estrutura, Fonte: Autor

A computação em nuvem é definida como um conjunto de serviços de computação, incluindo servidores, armazenamento, bases de dados, *networking*, software, analíticas e inteligência através da Internet (a nuvem) para oferecer inovação mais rápida, recursos flexíveis e economias de escala, onde se paga apenas pelos serviços que se utiliza na nuvem, reduzindo os seus custos nas operações, gerir a infraestrutura de forma mais eficiente, e escalar, à medida que o negócio precisa de mudança (Microsoft, 2021).

2.2 Modelos de Serviço

A maioria dos serviços de computação em nuvem enquadra-se em quatro grandes categorias: infraestrutura como serviço (IaaS), plataforma como serviço (PaaS), "*Serverless"* e software como serviço (SaaS) (Microsoft, 2021).

Figura 2 Modelo de Implementação de Nuvem, Fonte: Microsoft, 2021

2.2.1 Software como Serviço (SaaS)

O SaaS permite que os utilizadores utilizem aplicações baseadas na nuvem, através da Internet, alguns exemplos: *e-mail*, calendário e ferramentas de escritório. O SaaS fornece uma solução de *software* numa base de *pay-as-you-go* a um fornecedor de serviços em nuvem. As infraestruturas, *middleware* e *software* estão localizados no centro de dados do prestador de serviços. O prestador de serviços gere o *hardware* e *software*, e com o contrato de serviço apropriado, irá garantir a disponibilidade e a segurança das aplicações e dos seus dados (Microsoft, 2021) (Issa, 2021) (Wulandari, Jonas, & Alwarits, 2020).

2.2.2 Plataforma como Serviço (PaaS)

O PaaS é um ambiente completo de desenvolvimento e implementação na nuvem, com recursos que lhe permitem entregar tudo, desde aplicações simples baseadas na nuvem até aplicações empresariais sofisticadas. O cliente aluga/ compra os recursos que precisa a um fornecedor de serviços em nuvem, numa base de pagar pelo que se utiliza, com acesso pela Internet segura, e foi concebido para suportar o ciclo de vida completo da aplicação web: desenvolvimento, teste, implementação, gestão e atualização. O PaaS permite evitar a despesa e complexidade da compra e gestão de licenças de *software*, a infraestrutura de aplicações subjacentes e *middleware*, *kubernetes*, ou as ferramentas de desenvolvimento e outros recursos. O programador gere as aplicações e serviços que desenvolve, gerindo o fornecedor de serviços na nuvem, normalmente, tudo o resto (Microsoft, 2021) (Issa, 2021) (Wulandari, Jonas, & Alwarits, 2020).

2.2.3 Infraestrutura como Serviço (IaaS)

O IaaS é um tipo de serviço de computação em nuvem que oferece recursos essenciais de computação, armazenamento e *networking* a pedido, numa base de paga-se pelo o que se usar /consumir, e é um dos quatro tipos de serviços em nuvem, juntamente com o software como serviço (SaaS), plataforma como serviço (PaaS) e *Serverless*. Migrar a infraestrutura da sua organização para uma solução IaaS ajuda a reduzir a manutenção do *datacenter*, a economizar nos custos de *hardware* e a visualizar o negócio em tempo real.

As soluções IaaS dão-lhe a flexibilidade para escalar os seus recursos de Tecnologias de Informação (TI) para cima e para baixo, consoante a procura. Também o ajudam a providenciar rapidamente novas aplicações, e a aumentar a fiabilidade da sua infraestrutura subjacente. O IaaS permite-lhe contornar o custo e a complexidade da compra e gestão de servidores físicos e infraestrutura de *datacenter*. Cada recurso é oferecido como um componente de serviço separado, e só é pago por um recurso particular durante o tempo que se necessita (Microsoft, 2021) (Issa, 2021) (Wulandari, Jonas, & Alwarits, 2020).

2.2.4 *Serverless*

Permite que os programadores construam aplicações de forma rápida, eliminando a necessidade de gerir a infraestrutura. O fornecedor de serviços em nuvem, automaticamente, escala e gere a infraestrutura necessária para executar o código. A expressão "*serverless*" deriva do facto de as tarefas associadas ao fornecimento e gestão de infraestruturas serem invisíveis para o programador. Esta abordagem permite que os programadores aumentem o seu foco na lógica de negócio e entreguem mais valor ao núcleo do negócio. O "*serverless*" ajuda as equipas a aumentar a sua produtividade, a trazer produtos para o mercado mais rapidamente, e permite que as organizações otimizem os recursos e se mantenham focadas na inovação (Microsoft, 2021) (Wulandari, Jonas, & Alwarits, 2020).

2.3 Modelo de Implementação

A computação em nuvem é uma nova fase da evolução da Internet, que fornece as ferramentas para alterar a computação baseada em computação infraestrutural. Existem vários modelos, e cada um é usado com base na sua aplicação. Estes modelos incluem nuvens privadas, públicas, comunitárias e híbridas (Microsoft, 2021) (Wulandari, Jonas, & Alwarits, 2020).

2.3.1 Nuvem Privada

Consiste numa infraestrutura de computação em nuvem, estabelecida por uma organização para o seu uso interno. A nuvem privada realiza o funcionamento dentro das *firewalls* de uma organização, permitindo-lhe gerir de forma eficaz as infraestruturas internas de TI e fornecer serviços para os utilizadores locais. As nuvens privadas têm problemas de manutenção. Uma solução média, para eliminar problemas de nuvem privada e usar benefícios é usar nuvem privada virtual. Uma nuvem privada virtual é uma parte da infraestrutura de uma nuvem pública, como sendo aplicada para o uso privado de uma organização, e está disponível apenas por rede privada virtual (Taghipour, Mowloodi, Mahboobi, & Abdi, 2020) (Issa, 2021) (Wulandari, Jonas, & Alwarits, 2020).

2.3.1.1 Vantagens

Estas são as vantagens da nuvem privada (Microsoft, 2021):

- **Maior Flexibilidade** — uma organização pode personalizar o seu ambiente em nuvem para atender às necessidades específicas do negócio.
- **Maior Controlo —** os recursos não são partilhados com outros, por isso níveis mais elevados de controlo e privacidade são possíveis.
- **Maior Escalabilidade** — as nuvens privadas, muitas vezes, oferecem mais escalabilidade em comparação com a infraestrutura no local.

2.3.2 Nuvem Comunitária

A infraestrutura na nuvem é fornecida para consumidores exclusivos de uma comunidade e organizações que partilham preocupações. Pode ser de propriedade gerida e operada por uma ou mais organizações, um terceiro ou alguma combinação deles e pode existir dentro ou fora das instalações (Taghipour, Mowloodi, et al., 2020).

2.3.3 Nuvem Pública

Os serviços são prestados dinamicamente através da Internet e, como forma escalável, um fornecedor de terceiros e o fornecedor divide recursos e envia fatura calculada numa base de utilidade semelhante à indústria elétrica e telefónica. A *Google App Engine* e o

Serviço *Web* da Amazon são exemplos deste tipo de serviços (Taghipour, Mowloodi, et al., 2020) (Issa, 2021).

2.3.3.1 Vantagens

Estas são as vantagens sobre a nuvem pública (Microsoft, 2021):

- **Custos Mais Reduzidos** — não é necessário comprar hardware ou software e paga-se apenas pelo serviço que utiliza;
- **Sem Manutenção** — o seu fornecedor de serviços fornece a manutenção;
- **Escalabilidade Quase Ilimitada** — os recursos a pedido estão disponíveis para atender às necessidades do seu negócio;
- **Alta Fiabilidade** — uma vasta rede de servidores é um garante contra falhas.

2.3.4 Nuvem Híbrida

É uma junção de nuvem pública e privada e é uma escolha popular para a maioria das empresas, através da combinação de alguns serviços na nuvem, podendo os utilizadores, facilitar a transferência para a nuvem pública, através da eliminação de alguns problemas como sejam a consistência com padrões de segurança de dados de cartão de pagamento (Taghipour, Mowloodi, et al., 2020) (Issa, 2021).

2.3.4.1 Vantagens

Os seguintes tópicos são tidos como vantagens de uma nuvem híbrida (Microsoft, 2021):

- **Controlo** — a organização pode manter uma infraestrutura privada para ativos sensíveis ou cargas de trabalho que requerem baixa latência;
- **Flexibilidade** — pode aproveitar recursos adicionais na nuvem pública quando precisar deles;
- **Custo** — com a capacidade de escalar para a nuvem pública, paga-se pelo poder de computação extra apenas quando é necessário;

- **Facilidade** — a transição para a nuvem pode ser gradual, faseando-se em cargas de trabalho ao longo do tempo.

2.4 Benefícios

A computação em nuvem foi definida como uma grande mudança da forma tradicional como as empresas usam os recursos de TI. Nas alíneas seguintes estão as razões mais comuns, pelas quais as organizações estão a mudar para serviços de computação em nuvem (Microsoft, 2021) (Khan & Srivastava, 2018).

2.4.1 Custo

A computação em nuvem elimina a despesa de capital na compra de *hardware* e *software* e na criação e execução de *datacenters* no local, os *racks* dos servidores, a eletricidade vinte e quatro horas por dia para o arrefecimento e os especialistas em TI para gerir a infraestrutura (Microsoft, 2021) (Khan & Srivastava, 2018).

2.4.2 Velocidade

A maioria dos serviços de computação em nuvem são prestados em regime de *self-service* e a pedido, pelo que, mesmo grandes quantidades de recursos informáticos podem ser aprovisionadas em minutos, tipicamente com apenas alguns cliques de rato, dando às empresas muita flexibilidade e tirando a pressão do planeamento da capacidade (Microsoft, 2021) (Khan & Srivastava, 2018).

2.4.3 Escala Global

Os benefícios dos serviços de computação em nuvem, incluem a capacidade de escalar elasticamente, isso significa fornecer a quantidade certa de recursos de TI como, por exemplo, maior ou menor poder de computação, armazenamento, largura de banda quando são necessários e a partir da localização geográfica certa (Microsoft, 2021) (Khan & Srivastava, 2018).

2.4.4 Produtividade

Os centros de dados no local, normalmente, requerem uma grande quantidade de *racking and stacking*, configuração de *hardware*, *patching de software* e outras tarefas demoradas de gestão de TI. A computação em nuvem remove a necessidade de muitas destas tarefas, para que as equipas de TI possam gastar tempo a alcançar objetivos de negócio mais importantes (Microsoft, 2021) (Khan & Srivastava, 2018).

2.4.5 Desempenho

Os maiores serviços de computação em nuvem funcionam numa rede mundial de *datacenters* seguros, que são regularmente atualizados para a última geração de *hardware* de computação rápida e eficiente. Isto oferece vários benefícios sobre um único centro de dados corporativo, incluindo a redução da latência da rede para aplicações e maiores economias de escala (Microsoft, 2021) (Khan & Srivastava, 2018).

2.4.6 Fiabilidade

A computação em nuvem torna as cópias de segurança de dados, a recuperação de desastres e a continuidade do negócio mais fácil e menos dispendiosa, porque os dados podem ser espelhados em vários *sites* redundantes na rede do fornecedor de nuvem (Microsoft, 2021) (Khan & Srivastava, 2018).

2.4.7 Segurança

Muitos fornecedores de nuvem oferecem um vasto conjunto de políticas, tecnologias e controlos que fortalecem a sua postura de segurança em geral, ajudando a proteger de potenciais ameaças, os seus dados, aplicações e infraestruturas (Microsoft, 2021) (Khan & Srivastava, 2018).

2.5 Características Essenciais

Com base na definição de computação em nuvem existem várias características essenciais deste tipo de computação, sendo estas as principais características (Salehi, Noori, & Saboori, 2019) (Khan & Srivastava, 2018):

- **Agilidade** — a agilidade da nuvem funciona no modo distribuído e partilha os recursos entre os utilizadores sendo o seu desempenho muito rápido;

- **Atendimento de Serviço Automático** — a pedido, os fornecedores de computação em nuvem disponibilizam recursos, de acordo com os requisitos ou carga de trabalho desejados pelos consumidores, podendo os utilizadores aceder aos serviços da nuvem através da Internet;

- **Rápida Elasticidade** — os serviços da nuvem são elasticamente aprovisionados, para que o cliente possa adicionar ou remover novos serviços conforme a necessidade;

- **Fiabilidade** — na área da nuvem, a disponibilidade de servidores é muito alta e mais fiável, porque as probabilidades de falha de infraestruturas são mínimas. No caso de qualquer falha num dos servidores, haverá sempre uma cópia de segurança desses dados em outro servidor;

- **Serviço Medido** — o uso de recursos pode ser monitorizado, controlado e reportado, proporcionando transparência tanto para o fornecedor como para consumidor do serviço utilizado;

- **Amplo Acesso à Rede** — os recursos armazenados na nuvem podem ser acessíveis ou disponíveis para acesso a diferentes tipos de dispositivos, tais como telemóveis, computadores portáteis, *tablets*, etc. de onde quer que estejam ligados à Internet a que possam aceder amplamente à rede.

3 Privacidade dos Dados na UE

O Regulamento Geral de Proteção de Dados (RGPD), é um diploma da União Europeia, que protege e regula o tratamento indevido dos dados, de todos os cidadãos europeus. Uma segunda definição de RGPD consiste na harmonização do grau de proteção de dados em todos os países de UE, introduzindo uma única lei transversal a todos os estados-membros. A intenção é trazer mais e melhor transparência, para o processamento dos dados de um indivíduo e impulsionar a economia digital dos estados-membros e participantes (Mammona, Kanwal, et al., 2019). Apesar de ter sido redigido e aprovado pela UE, impõe obrigações às organizações em qualquer lugar do mundo, desde que direcionem ou recolham dados relacionados com as pessoas na UE *(AG, Horizon 2020 Framework Programme of the European Union and Proton Technologies, 2021*).

O RGPD não só pretende dar aos cidadãos e residentes da União Europeia (UE) e do Espaço Económico Europeu (EEE) o controlo sobre os seus dados pessoais, simplificando a regulação ambiente para as empresas internacionais e harmonizando totalmente as leis nacionais de dados dos seus Estados-Membros, como também tem o objetivo de criar uma abordagem coerente e abrangente, tanto para as violações da privacidade como para a vigilância em massa dos cidadãos da UE (Baker, 2019).

A execução do RGPD é realizada através da Supervisão de Autoridades (SAs). Cada Estado-Membro da UE nomeia uma SA, todas coordenadas pelo Conselho Europeu de Proteção de Dados que tem a autoridade para realizar auditorias, emitir advertências, multas, impor limites ou proibições ao processamento, entre outras competências (Chorpash, 2020).

O tratamento de dados pessoais tem o mesmo significado nos termos da Diretiva 95/46/CE e do RGPD. É definido no RGPD da seguinte forma: qualquer operação ou conjunto de operações que seja efetuada em dados pessoais ou em conjuntos de dados pessoais, seja por meios automatizados, tais como recolha, gravação, organização, estruturação, armazenamento, adaptação ou alteração, recuperação, consulta, utilização, divulgação por transmissão, divulgação ou disponibilização, alinhamento ou combinação, restrição, apagamento ou destruição (Stendal, 2020).

No âmbito do RGPD, a pseudónimo arrisca a reidentificação dos titulares dos dados e é descrita da seguinte forma: o tratamento de dados pessoais, para que os mesmos deixem de poder ser atribuídos a um titular de dados específicos, sem a utilização de informações adicionais, desde que essas informações adicionais sejam mantidas separadamente e estejam sujeitas a medidas técnicas e organizativas para garantir que os dados pessoais não sejam atribuídos a uma pessoa singular identificada ou identificável (Stendal, 2020).

As categorias de dados pessoais, foram adicionadas ao abrigo do RGPD, tais como dados de localização e identificadores *online*. Os identificadores *online* são identificadores fornecidos por dispositivos, aplicações, ferramentas e protocolos de pessoas singulares, tais como endereços de Protocolo de Internet (IP), identificadores de *cookies* ou outros identificadores, tais como etiquetas de identificação de frequência de rádio. Quando combinados com identificadores únicos, os identificadores *online* podem ser usados para criar perfis de pessoas naturais e identificá-los (Stendal, 2020).

3.1 História

O direito à privacidade faz parte da Convenção Europeia dos Direitos Humanos de 1950, na qual se estabelece que todos têm o direito de respeitar a sua vida privada e familiar, a sua casa e a sua correspondência. Desta forma, a União Europeia procurou assegurar a proteção deste direito através da legislação. Com o desenvolvimento tecnológico e a invenção de Internet, a UE chegou à conclusão que há uma necessidade de assegurar as proteções modernas (*AG, Horizon 2020 Framework Programme of the European Union and Proton Technologies, 2021*).

O RGPD foi precedido por duas diretivas-chave relativas à proteção de dados: a primeira foi da OCDE, de 1980 (Recomendações do Conselho Sobre as Orientações que gerem a Proteção da Privacidade e do Fluxo Transfronteiriço de Dados Pessoais) e a segunda foi a Diretiva relativa à proteção de dados da EU, de 1995 (Diretiva) que foi construída sobre os sete princípios: (1) Os indivíduos devem ser notificados quando os seus dados pessoais são recolhidos; (2) a recolha deve ser limitada e, com o consentimento do titular dos dados; (3) a recolha de dados deve ser relevante, atualizada e, para uma finalidade específica; (4) os dados não devem ser divulgados, exceto com o consentimento do utilizador ou por razões legais; (5) os dados devem ser protegidos por

salvaguardas de segurança; (6) os titulares dos dados devem ter o direito de ter informações sobre os dados recolhidos sobre os mesmos e (7) os responsáveis pelos tratamentos de dados pessoais devem ser responsabilizados pelo cumprimento das leis gerais contidos nas recomendações da OCDE sobre proteção da privacidade (Khan B. D., 2020).

Em outubro de 1995, foi aprovado pela Diretiva Europeia de Proteção de Dados, a lei estabelece assim normas mínimas de privacidade e segurança de dados, sobre as quais cada membro da UE baseou a sua própria lei de execução (*AG, Horizon 2020 Framework Programme of the European Union and Proton Technologies, 2021*). O objetivo desta diretiva era o de salvaguardar os dados pessoais do indivíduo. A diretiva foi implementada em outubro de 1998 como parte importante do direito da privacidade e dos direitos humanos da UE. As Leis de Proteção de Dados de 1988 e 2003 conferem direitos às pessoas, e colocam responsabilidades sobre os ombros daqueles que tratam dados pessoais *(Mammona, Kanwal, Fleury, Herbst, & Qiao, 2019)*. Ainda em 1995, a Comunidade Europeia adotou, por conseguinte, a Diretiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de outubro de 1995 relativa à proteção das pessoas no tratamento de dados pessoais e à livre circulação desses dados (Bussche, 2017).

A Diretiva relativa à proteção de dados tinha duas versões de projeto: a Proposta Original e a Proposta Alterada, publicada em conjunto com um Memorando explicativo da Comissão Europeia (Moerel, 2011). Na proposta original, o fator de ligação para a escolha da legislação nacional aplicável era a localização do ficheiro de dados.

No que diz ser necessário evitar a aplicabilidade das leis de privacidade da UE, a proposta original previa que a transferência de um ficheiro de dados, por parte de um responsável pela EU para um país terceiro, não fosse impedir a proteção das leis de privacidade da UE (Moerel, 2011).

Diversos eventos fizeram com que o processo de aprovação de RGPD fosse mais célere que o normal, conforme se segue: em 1994, o primeiro anúncio de *banner* apareceu online; em 2000 a maioria das instituições financeiras ofereciam acesso às suas contas online; em 2006 o Facebook abriu ao público e em 2011 um utilizador do Google processou a empresa por digitalizar os seus e-mails (*AG, Horizon 2020 Framework Programme of the European Union and Proton Technologies, 2021*). O RGPD entrou em vigor em 2016, após a aprovação do Parlamento Europeu, e a partir de 25 de maio de 2018, todas as organizações foram obrigadas a cumprir.

3.1.1 RGPD — Diretiva Europeia de Proteção de Dados

O RGPD cumpre os seus dois objetivos com muitos ajustamentos das diretivas anteriores, alguns ligeiros e alguns substanciais. Estabelece novos requisitos no domínio da proteção de dados, notificação de violação de dados, limites sobre o tratamento, transparência, direitos de privacidade de dados e limites aos dados transferência para fora da UE (Chorpash, 2020). Embora as diretivas anteriores da UE previssem alguns direitos como direitos de acesso, retificação, eliminar e portabilidade de dados, o RGPD cria novos direitos para os utilizadores, tais como o direito ao apagar e de ser esquecido (Chorpash, 2020). Existem requisitos de segurança adicionais que as empresas devem cumprir. O RGPD determina um nível de segurança adequado para os dados pessoais recolhidos pelas empresas, incluindo a proteção contra o processamento ilícito, danos, destruição, ou perda acidental.

Estes fatores são importantes, para as empresas contemplarem e desenharem sistemas para salvaguardar os dados dos utilizadores; um dos requisitos do RGPD inclui criar uma Avaliação do *Data Protection Impact Assessment* (DPIA) conduzido pelo *Data Protection Officer* (DPO). Antes de o RGPD ser implementado, muitas empresas tiveram uma busca incansável de alguém que desempenhasse bem a função de DPO (Chorpash, 2020). Em comparação com a diretiva anterior sobre a proteção de dados da UE, o RGPD representa uma intensificação significativa do ambiente jurídico, na sua obrigação para todos os Estados-Membros e inclui os direitos de apagar e aceder, requisitos por consentimento afirmativo, bem como a capacidade de cobrar multas pesadas (Baker, 2019).

3.2 Princípios Básicos de Processamento

O RGPD assume que, por padrão, os controladores de dados desejam recolher e processar conjuntos de dados pessoais ou identificados. Nestes casos, o RGPD exige que os controladores de dados sigam alguns princípios, que trabalham em conjunto para formar uma rede de proteção de dados para os salvaguardar. Inicialmente, focou-se na recolha e minimização de dados e categorias especiais; os dois seguintes dizem respeito ao processamento de dados: especificação de propósito e decisões automatizadas (Baker, 2019).

3.2.1 Minimização dos Dados

Para aprovar o princípio da minimização dos dados, o RGPD exige que as recolhas dos dados se limitem ao necessário, em relação às finalidades para as quais são processadas. Na verdade, o princípio da minimização de dados é intuitivo, na limitação da recolha de um conjunto de dados, o que significa que os responsáveis pelos tratamentos de dados têm opções limitadas (Baker, 2019) (Gazis, 2021).

Adicionalmente, a classificação adequada e políticas claras sobre o tratamento de dados melhoram a qualidade dos dados e as saídas da ciência dos dados. Em qualquer caso, as soluções de proteção de dados por design podem implicar anonimização, quando possível, quando o armazenamento de dados pessoais não é justificável (Gazis, 2021). Segundo Zarsky (2016), os dados são considerados pessoais se se referir ou descrever, com precisão, alguns aspetos de um indivíduo vivo e identificável; o RGPD proíbe a partilha de dados, tais como: nome, localização, números de identificação, endereço IP e informação económica sendo considerados de dados pessoais, e devem ser limitados ao princípio de minimização de dados (Baker, 2019) (Gazis, 2021).

3.2.2 Precisão

Segundo Rania El-Gazzar and Karen Stendal 2020, os dados pessoais devem ser exatos e, se necessário, mantidos atualizados; devem ser dados todos os passos razoáveis para garantir que os dados pessoais inexatos, tendo em conta as finalidades para as quais são tratados, sejam apagados ou retificados sem demora.

Outro objetivo do princípio da precisão, consiste em assegurar uma limitação temporal da utilização de dados, para o período para o qual os dados pessoais são armazenados se limite a um mínimo estrito, e que os prazos devem ser estabelecidos pelo controlador para a eliminação ou para uma revisão periódica (Baker, 2019).

O RGPD alerta também contra qualquer utilização não reconhecida de decisões automatizadas no tratamento de dados. O princípio não proíbe a automação, mas num esforço para preservar os direitos dos indivíduos sujeitos a estes processos, requer que as empresas obtenham o seu consentimento explícito, se quiserem usar estas técnicas (Baker, 2019). Além disso, o consentimento dos sujeitos aos dados deve ser dado livremente, específico, informado e inequívoco. Os utilizadores devem saber exatamente pelo que estão a optar, e não podem ser induzidos em erro. As empresas também devem informar os clientes ou as pessoas envolvidas, dos seus direitos de retirar o seu consentimento a qualquer momento, e deve ser fácil para os utilizadores retirarem o mesmo dado inicialmente.

3.2.3 Legalidade, Justiça e Transparência

Isso significa que, para além da identificação da base jurídica relevante, os intervenientes devem assegurar que o tratamento de dados seja justo e transparente. Ao realizar uma grande análise de dados, o objetivo constitui um fator importante para avaliar os princípios da justiça e da transparência. Os indivíduos são informados sobre a utilização prevista dos seus dados, numa linguagem simples e clara (Gazis, 2021). A justiça está ligada à questão de saber se os dados serão tratados de forma esperada, sem causar efeitos adversos injustificados, sem causar danos individualmente ou em grupo. Igualmente, as vulnerabilidades devem ser consideradas ao avaliar o nível provável de entendimento do indivíduo. A falta de transparência pode implicar que os indivíduos não tenham ideia ou controlo, sobre a forma como os seus dados são utilizados (Gazis, 2021).

3.2.4 Limite de Armazenamento

Quanto ao limite de armazenamento, os grandes exemplos de dados para a COVID-19 têm um objetivo específico: limitar a propagação do vírus e proteger a saúde pública. No entanto, a reutilização dos dados pessoais recolhidos durante a assistência humanitária pode colocar este princípio sob pressão. Com base no artigo 5.º do RGPD, os dados

pessoais devem ser recolhidos para fins específicos, explícitos e legítimos e não posteriormente tratados de forma incompatível com essas finalidades (Gazis, 2021).

Este princípio, permite que os indivíduos façam uma escolha informada sobre a recolha dos seus dados ao ator auxiliar, e certificarem-se de que os mesmos não serão processados para fins irrelevantes, sem o seu consentimento ou conhecimento. Em todo o caso, a finalidade deve ser clara e legítima, ou seja, deve existir uma ligação objetiva entre a finalidade do tratamento e as atividades do responsável pelo tratamento de dados (Gazis, 2021) (Mammona, Kanwal, et al., 2019). Karen Stendal 2020, defende que os dados pessoais devem ser conservados para permitir a identificação de pessoas sujeitas a um tempo não superior ao necessário para as finalidades para as quais os dados pessoais são tratados, os quais podem ser armazenados por períodos mais longos, na medida em que serão tratados, exclusivamente, para fins de investigação científica ou histórica, ou fins estatísticos, sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo RGPD, a fim de salvaguardar os direitos e liberdades do titular dos dados.

3.2.5 Confidencialidade e Integridade

A confidencialidade é um dos princípios-chave, o que significa que os dados devem ser suficientemente protegidos contra a divulgação não autorizada. A segurança dos dados também é conseguida aplicando os princípios de minimização de dados e a limitação do armazenamento, visto que a diminuição da recolha reduz o risco de violações de dados (Gazis, 2021). A encriptação e o pseudónimo dos conjuntos de dados bem como a substituição de identidades pessoais por códigos, são também promovidos pelo RGPD como uma medida de segurança, que pode impedir o uso indevido de dados (Gazis, 2021).

Os dados recolhidos devem manter a sua integridade e confidencialidade. Os controladores devem utilizar as medidas técnicas adequadas para fornecer segurança adequada dos dados pessoais, incluindo a proteção contra o tratamento ilícito ou a perda acidental, destruição ou dano (Mammona, Kanwal, et al., 2019.

3.2.6 Prestação de Contas

Os controladores devem ser responsabilizados se o tratamento de dados for não conforme com os princípios da cláusula 5.1(a-f). O artigo 6.º diz respeito à licitude do tratamento, fornecendo um formulário de consentimento adequado para o titular dos dados para o tratamento dos mesmos. O processamento deve ser feito mantendo as obrigações legais em mente; a alínea e do artigo 6.º, menciona as salvaguardas adequadas para os dados pessoais, utilizando os procedimentos de encriptação ou pseudónimo. A alínea f do artigo 6.º esclarece ser permitido o tratamento legítimo de dados pelos responsáveis pelos tratamentos, exceto que este processo não deve sobrepor-se aos direitos e liberdade, especialmente se o titular dos dados for uma criança (Mammona, Kanwal, et al., 2019.

3.2.7 Limitação de Finalidade

Os dados pessoais devem ser recolhidos para fins específicos, explícitos e legítimos e não posteriormente tratados de forma incompatível com essas finalidades, não se considerando incompatível com os fins de investigação, no interesse público, científico ou histórico, nem para fins estatísticos, nem arquivos (Stendal, 2020).

3.3 Processamento de Dados Pessoais

Segundo o RGPD, o artigo 32.º é um artigo importante quando lidamos com o tratamento seguro de dados pessoais. Este artigo, salienta que o responsável pelo tratamento e pelos transformadores, deve aplicar as medidas técnicas e organizativas apropriadas, a fim de garantir um nível de segurança adequado para preservar os direitos e liberdades de um titular de dados (Mammona, Kanwal, et al., 2019).

O artigo 32.º descreve duas medidas de segurança quando lidamos com segurança e processamento dos dados pessoais; a primeira refere-se a:

- Pseudonimização e encriptação de dados pessoais;
- Assegurar que os procedimentos se aplicam em todos os serviços de segurança, isto é, confidencialidade, integridade, disponibilidade e resiliência;

- Em caso de emergência, rapidamente restaurando o acesso e disponibilidade de dados pessoais;

- Assegurar a avaliação e validação regulares dos procedimentos de segurança adotados para uma proteção eficaz da privacidade.

A segunda medida, assinala os riscos de transformação, isto é, destruição acidental e ilícita, perda, alteração e não autorizada divulgação de dados processados e armazenados. Estes riscos devem também ser avaliados juntamente com a avaliação da adequação dos níveis de segurança (Mammona, Kanwal, et al., 2019).

3.4 Princípios de Privacidade para a Proteção de Dados

O artigo 25.º descreve o princípio-chave da privacidade para todas as empresas, por outras palavras, a Proteção de Dados por *Design* e por defeito. Serve de espinha dorsal para as empresas, em conformidade com o RGPD, implementando a proteção da privacidade para os dados sensíveis de um titular de dados (Mammona, Kanwal, et al., 2019).

3.4.1 Proteção de Dados por Desenho

As medidas organizacionais e as técnicas adequadas para garantir a segurança e privacidade dos dados pessoais, estão incorporadas no ciclo de vida completo dos produtos, serviços, aplicações, procedimentos empresariais e técnicos de uma organização. As medidas técnicas propostas são pseudónimo e minimização de dados (Mammona, Kanwal, et al., 2019).

3.4.2 Proteção de Dados por Predefinição

Isto significa que: em primeiro lugar, apenas os dados pessoais necessários são recolhidos, armazenados ou tratados; e, em segundo lugar, os dados pessoais não são acessíveis por pessoas não autorizadas (Mammona, Kanwal, et al., 2019).

3.4.3 Certificação

A conformidade com a Proteção de Dados por requisitos de conceção e de predefinição, deve ser demonstrada através de uma certificação aprovada conforme indicado no artigo 42.º (Mammona, Kanwal, et al., 2019).

3.5 Direitos do Titular dos Dados

Os artigos 16.º a 18.º têm a ver com os direitos de retificar, apagar e restringir tratamento dos seus dados pessoais; assim sendo, são atribuídos os seguintes oito direitos aos titulares de dados sob a proteção do RGPD (Mammona, Kanwal, et al., 2019).

- Solicitar o acesso aos seus dados pessoais recolhidos por uma organização;
- Solicitar a eliminação dos seus dados pessoais recolhidos por uma organização;
- Solicitar a transferência dos seus dados pessoais de um prestador de serviços a outro;
- Ser informado sobre a recolha de dados;
- Atualizar ou corrigir quaisquer dados pessoais inválidos recolhidos pela organização;
- Proibir o tratamento dos seus dados;
- Negar a utilização dos seus dados pessoais para marketing;
- Ser notificado de uma violação de dados pessoais dentro de 72 horas da violação.

3.5.1 Direito de Acesso

No artigo 15.º, os titulares de dados têm direito de solicitar o acesso aos seus dados pessoais recolhidos e podem inquirir uma empresa sobre a utilização dos mesmos. A empresa é obrigada a fornecer uma cópia gratuita dos dados pessoais em formato eletrónico, mediante pedido (Mammona, Kanwal, et al., 2019).

3.5.2 Direito de Eliminar

No artigo 17.º, as empresas que fazem a recolha de dados devem eliminar os dados dos indivíduos que deixarem de ser seus clientes, ou que retiraram o seu consentimento, a uma empresa para utilizar os seus dados pessoais (Mammona, Kanwal, et al., 2019).

3.5.3 Direito de Transferência dos seus Dados

No artigo 20.º, os indivíduos têm o direito de transferir os seus dados de um prestador de serviços para outro (Mammona, Kanwal, et al., 2019).

3.5.4 Direito a ser Informado

O artigo 19.º, especifica que antes da recolha de quaisquer dados por empresas, os particulares devem ser informados. Os consumidores têm que optar pelos seus dados a serem recolhidos e o consentimento deve ser dado livremente, em vez de forma implícita (Mammona, Kanwal, et al., 2019).

3.6 Requisitos Organizacionais

3.6.1 Registos de Atividades de Processamento

Os controladores e os transformadores terão de implementar registos das suas atividades de processamento que, se forem mantidas minuciosamente, permitirão provar o cumprimento do RGPD perante as Autoridades de Supervisão e ajudar a preencher as informações e obrigações para com os sujeitos de dados. Os registos devem conter, nomeadamente, informações sobre as finalidades do tratamento, as categorias de dados afetados e uma descrição das medidas técnicas e organizacionais de segurança aplicadas. Fornecem detalhes sobre o conteúdo e propósito dos registos, bem como as — na prática, raramente aplicáveis — exceções a esta obrigação (Bussche, 2017).

3.6.2 Designação de um Oficial de Proteção de Dados

As entidades privadas são obrigadas a designar um oficial de Proteção de Dados, se as suas atividades fundamentais ou decisivas para a sua estratégia de negócio, consistirem na monitorização regular e sistemática de pessoas, ou no tratamento de categorias especiais de dados pessoais (como dados de saúde) em larga escala.

Grupos de empresas podem designar um único Oficial de Proteção de Dados, para a totalidade ou algumas das entidades do grupo. Qualquer oficial de proteção de dados deverá ser designado com base nas suas competências e qualidades profissionais, para garantir que possa desempenhar com sucesso as suas responsabilidades, tais como o acompanhamento do cumprimento da entidade pelo RGPD (Bussche, 2017).

Estas são as condições necessárias para nomear um Oficial de Proteção de Dados (AG, Horizon 2020 Framework Programme of the European Union and Proton Technologies, 2021):

- É uma autoridade pública que não atua num tribunal a título judicial;
- As suas atividades principais exigem que monitorize as pessoas de forma sistemática e regular em larga escala;
- As suas atividades fundamentais são o tratamento em larga escala de categorias especiais de dados enumerados no artigo 9.º do RGPD ou dados relativos a condenações penais e infrações referidas no artigo 10.º, como, por exemplo, um consultório médico.

3.6.3 Avaliação de Impacto da Proteção de Dados

Se uma atividade de tratamento pretendida, nomeadamente, utilizando novas tecnologias, resultar num risco elevado para os direitos e liberdades dos titulares dos dados, as entidades devem realizar uma avaliação preventiva do impacto da proteção de dados identificando as medidas adequadas para mitigar os respetivos riscos. Se os resultados da avaliação não permitirem que a entidade determine quais as salvaguardas que poderiam ser aplicadas, ter-se-á de consultar as Autoridades. Estas últimas poderão emitir, no futuro, listas a preto e branco, que clarifiquem quais as atividades de

processamento que exigirão uma avaliação de impacto da proteção de dados (Bussche, 2017).

3.6.4 Medidas Técnicas e Organizacionais

As entidades devem implementar medidas técnicas e organizacionais para garantir a salvaguarda dos dados pessoais. O nível adequado de proteção de dados deve ser determinado com base no potencial de risco inerente às atividades de tratamento da entidade numa base casuística (Bussche, 2017).

3.6.5 Sistema de Gestão de Proteção de Dados

Sempre que possível, com base no orçamento e nos recursos de uma entidade, o cumprimento do RGPD poderá ser implementado e monitorizado através de um Sistema de Gestão da Proteção de Dados. Trata-se de um sistema de conformidade interno que monitorizará o cumprimento dos requisitos relacionados com a proteção de dados e relacionados com a segurança (Bussche, 2017).

3.7 Justificações Legais para o Tratamento de Dados

As atividades de tratamento de dados, só podem ser lícitas se estiverem cobertas pelo consentimento do titular dos dados ou por uma autorização legal. Qualquer tratamento de dados, independentemente de se realizar dentro ou fora da UE, é proibido, a menos que seja abrangido por uma base jurídica (Bussche, 2017).

3.7.1 Processamento Baseado no Consentimento

Em comparação com a Diretiva relativa à Proteção de Dados, o RGPD estabelece requisitos mais rigorosos, para a obtenção de consentimento válido dos sujeitos de dados. Prevê igualmente, uma proteção jurídica mais forte das crianças. Além disso, o consentimento para o processamento de especiais categorias de dados pessoais está sujeito a requisitos ainda mais rigorosos. Assim, as entidades precisam de rever a sua prática de consentimento atual para o cumprimento do RGPD.

Segundo o art.º. 4.º do CGPD, o consentimento significa qualquer indicação livre, específica, informada e inequívoca dos desejos do titular dos dados pelo qual, por declaração ou por uma ação afirmativa clara, significa acordo para o tratamento dos seus dados pessoais (Bussche, 2017).

3.7.2 Processamento com Base numa Permissão Legal

Se a atividade de tratamento de dados não se basear no consentimento nos termos do art.º. 6.º, a licitude poderá decorrer de outra autorização legal prevista neste artigo do RGPD. É de notar que estas autorizações legais são formuladas de forma abstrata e estão parcialmente abertas à especificação pela legislação dos Estados-Membros da UE. Na prática, as entidades muitas vezes baseavam as suas atividades de processamento em várias bases legais. Por exemplo, quando uma entidade processa dados pessoais com base na sua necessidade de realização de um contrato, essa entidade também obteria frequentemente o consentimento do titular dos dados. Esta abordagem preventiva visa assegurar a legalidade das operações de transformação no caso de uma ou várias das bases jurídicas utilizadas perderem a sua legitimidade. Esta abordagem pode ser mantida no âmbito do RGPD (Bussche, 2017).

3.8 Coimas por Violar as Leis

As coimas do RGPD destinam-se tanto para as grandes como para as pequenas empresas, que cometam o erro de não respeitar as regras impostas (*AG, Horizon 2020 Framework Programme of the European Union and Proton Technologies, 2021).* Os dois níveis de coimas do RGPD são: as infrações menos graves, que podem resultar numa coima até 10 milhões de euros equivalente a 2% ou até 20 milhões de euros, equivalente a 4% das receitas anuais da empresa do exercício anterior e segundo.

As coimas mais leves, incluem violações como: organizações com a função de Controladores ou Processadores, Organismos de certificação e de monitorização enquanto as mais pesadas são: os princípios básicos de processamento, as condições de consentimento, os direitos dos titulares de dados e a transferência de dados para uma organização internacional (*AG, Horizon 2020 Framework Programme of the European Union and Proton Technologies, 2021*).

3.9 Outros Conceitos

3.9.1 Dados Pessoais

Consistem em qualquer informação que se relacione com um indivíduo, com a qual possa ser identificado direta ou indiretamente. Nomes, endereços de e-mail, informações de localização, etnia, sexo, dados biométricos, crenças religiosas, cookies web e opiniões políticas, são considerados dados pessoais (*AG, Horizon 2020 Framework Programme of the European Union and Proton Technologies, 2021*).

3.9.2 Processamento de Dados

Qualquer ação realizada em dados, de forma automática ou manual; referem-se como exemplos: a recolha de informação, gravação, organização, estruturação, armazenamento, utilização e eliminação (*AG, Horizon 2020 Framework Programme of the European Union and Proton Technologies, 2021*).

3.9.3 Titular de Dados

A pessoa cujos dados são tratados; podem ser clientes ou visitantes do site (*AG, Horizon 2020 Framework Programme of the European Union and Proton Technologies, 2021)*.

3.9.4 Controlador de Dados

A pessoa que decide como os dados pessoais serão tratados e se é proprietário ou empregado na sua organização que trata dados (*AG, Horizon 2020 Framework Programme of the European Union and Proton Technologies, 2021*).

3.9.5 Processador de Dados

Pode ser considerado um terceiro que processa dados pessoais em nome de um controlador de dados; o RGPD tem regras especiais para estes indivíduos e organizações, que incluem servidores num fornecedor de nuvem ou como fornecedores de serviços de e-mail, como sejam o Outlook ou Gmail (*AG, Horizon 2020 Framework Programme of the European Union and Proton Technologies, 2021*).

4 Privacidade dos Dados nos EUA

Os Estados Unidos têm uma abordagem diferente das leis de proteção de dados pessoais aplicáveis às empresas privadas. Com exceção dos estatutos federais específicos da indústria, a maioria dos regulamentos de proteção de dados aplicáveis às empresas têm origem no Estado. E respondendo a enormes violações de dados, os legisladores estaduais começaram a elaborar e a aprovar projetos de lei de privacidade de dados trans-jurisdicionais, que regulam o uso de informações pessoais (Ventura, 2020). A razoabilidade é determinada pelo equilíbrio de dois interesses importantes: primeiro, a intrusão nos direitos da Quarta Emenda de um indivíduo e, segundo, o legítimo interesse do governo na segurança pública (Barrett, 2019). Como exemplo, buscas e apreensões dentro de uma casa sem mandado são presuntivamente inaceitáveis, mas se a busca for incidente a uma prisão legal, pode não haver necessidade de um mandado. Assim, nos EUA, o direito à privacidade é baseado em contextualização e no âmbito limitado (Barrett, 2019).

Há algumas leis federais dos EUA que reconhecem o direito à privacidade e proteção de dados fora da Quarta Emenda. No entanto, estas leis são geralmente limitadas em âmbito a sectores específicos. Por exemplo, a *GrammLeach-Bliley Act* aplica-se à indústria financeira e fornece proteções de privacidade de dados estritamente adaptadas em circunstâncias específicas. Outro exemplo é o *Health Insurance Portability and Accountability Act* (HIPAA), que procura salvaguardar as informações de saúde individualmente identificáveis sob qualquer forma: eletrónica, papel ou oral (Barrett, 2019).

4.1 História das Leis de Privacidade

Foi em 1890, quando Warren e Brandeis (in Houser, 2019) escreveram um importante artigo sobre o direito à privacidade e argumentaram que o mesmo está implícito e derivado tanto do direito à vida como do direito comum. Estes direitos foram alargados, para incluir o direito de manter certas informações pessoais fora do domínio público (Ventura, 2020).

Pouco tempo depois da publicação do artigo do Warren e Brandeis, em 1903, Nova Iorque aprovou um estatuto de privacidade, que prevê a causa da ação por violações da

privacidade. Em 1905, o Supremo Tribunal da Geórgia reconheceu uma violação do direito comum à invasão da privacidade, argumentando que o direito à privacidade se baseia nos instintos da natureza reconhecido intuitivamente. Outros Estados incluíam, afirmativamente, o direito à privacidade nas suas constituições.

Em 1960, o Reitor William Prosser (in Ventura 2020), analisou as decisões de privacidade do tribunal estatal após o artigo de Warren e Brandeis (in Ventura 2020), tendo dividido os casos em quatro categorias:

- Intrusão no isolamento;
- Divulgação pública de factos embaraçosos;
- Publicidade colocada em falsa luz;
- Apropriação da sua imagem ou semelhança.

A Reafirmação de Torts adotou a tipologia do Reitor Prosser (in Ventura, 2020), reconhecendo tais *torts* coletivamente como invasão de privacidade.

Embora muitos tribunais estatais tenham aceite os quatro delitos de privacidade, fizeram-no em diferentes pontos e graus (apenas o Dakota do Norte ainda não reconheceu nenhum dos quatro delitos de privacidade do direito comum) (Ventura, 2020).

No entanto, o poder judicial federal interpretou separadamente e simultaneamente os interesses de privacidade dos dados nos termos da Constituição, tendo o Supremo Tribunal abordado a constitucionalidade das tecnologias emergentes e a ameaça que impuseram à privacidade dos dados pessoais nas mãos da aplicação da lei (Ventura, 2020).

Nos Estados Unidos, o Congresso decidiu deliberadamente não aprovar a regulamentação de dados no ano de 1970, a fim de preservar e proteger a inovação e as liberdades económicas. Segundo a maioria das leis de privacidade de dados dos EUA, as empresas não estão proibidas de processar dados pessoais ou são obrigadas a minimizar o tratamento de dados, sendo apenas obrigadas a respeitar restrições estritamente adaptadas consideradas necessárias para proteger privacidade individual (Gupta, 2019).

O Supremo Tribunal da Califórnia abriu esta exceção, no que diz respeito ao direito do Estado à privacidade em reconhecimento de uma iniciativa de escrutínio de 1972, através da qual o povo da Califórnia adicionou o direito à privacidade à Constituição da Califórnia. Na prática, o direito constitucional do Estado à privacidade não adicionou quaisquer regras ou proibições substantivas ao já robusto e detalhado órgão da lei de privacidade da Califórnia (Gupta, 2019). A Califórnia tem uma abordagem diferente do direito constitucional à privacidade e interpreta o direito de forma mais ampla. Em 1994, o Supremo Tribunal da Califórnia considerou que o direito à privacidade no artigo 1.º, secção 1 da Constituição da Califórnia, se aplica a empresas privadas, embora outros direitos civis concedidos pela Constituição da Califórnia, geralmente se apliquem apenas em relação ao Estado (Gupta, 2019).

Com a implementação de CCPA em 2018, as empresas têm que solicitar o consentimento prévio não só dos menores como dos seus pais, antes de vender informações pessoais relativas a crianças com menos de 16 anos.

Caso contrário, o tratamento de dados pessoais não é proibido ou limitado, a menos ou até que um titular de dados exija o seu direito ao abrigo do CCPA de limitar o tratamento de informações individuais (Gupta, 2019).

Inspirada, em parte, pelo RGPD, a legislação sobre a privacidade dos dados do estado ameaça consolidar os mercados entre as grandes empresas capazes de cumprir os regulamentos e impor normas contraditórias às indústrias baseadas na tecnologia e na Internet que abrangem jurisdições e são fundamentais para a economia dos EUA, onde se propõe uma solução regulamentar, para abordar as preocupações de privacidade dos dados pessoais no âmbito das práticas comerciais das empresas tecnológicas. A solução contempla um organismo autorregulador que (Ventura, 2020):

- Promulga as normas da indústria;
- Diferencia as grandes e as pequenas empresas baseadas na Internet;
- Cria maior transparência em torno da utilização dos dados dos consumidores.

A solução deixa a aplicação da lei para a *Federal Trade Comission (FTC)*, o organismo encarregue de julgar as violações das leis de privacidade existentes. O

mecanismo de aplicação da lei atinge um equilíbrio que carece das duas principais propostas de legislação federal abrangente e legislação estatal para proteções de privacidade de dados pessoais (Ventura, 2020).

4.1.1 A Quarta Emenda

A Quarta Emenda à Constituição, destinada a prevenir buscas e apreensões irrazoáveis, prevê, em parte pertinente que o direito das pessoas a estarem seguras nas suas casas contra buscas e apreensões irrazoáveis, não deve ser violado. O Supremo Tribunal reconhece a intenção dos Fundadores, de garantir aos cidadãos que o direito de ser muito mais abrangente do que qualquer direito à intrusão injustificável do governo sobre a privacidade do indivíduo, independentemente do meio utilizado, deve ser considerado uma violação da Quarta Emenda (Ventura, 2020).

A Quarta Emenda não prevê um direito constitucional geral à privacidade. Em vez disso, protege a privacidade individual contra certos tipos de intrusões governamentais. A Quarta Emenda protege as pessoas de buscas e apreensões por parte do governo, mas não garante um direito geral à privacidade (Barret, 2019).

4.1.2 Indústria de Seguros e Saúde: HIPAA

A Regra da Privacidade aplica-se a entidades abrangidas, nomeadamente, planos de saúde, centros de compensação de cuidados de saúde e prestadores de cuidados de saúde. Protege informações orais e gravadas sobre o passado, presente ou doenças futuras do paciente. As entidades abrangidas são escolas, autoridades de saúde pública, seguradoras e empregadores, que podem criar esta informação.

E a informação relevante mantém as suas proteções HIPAA, à medida que passa das mãos de entidades abrangidas para outras entidades abrangidas ou não abrangidas (Ventura, 2020).

A regra de privacidade, proíbe entidades abrangidas de divulgar dados de saúde protegidos sem autorização. A pessoa a quem os registos se referem deve autorizar a divulgação por escrito e indicar informação aos destinatários. A autorização deve ter uma data de validade, após a qual o destinatário já não pode aceder à informação. Por último,

a Regra de Privacidade proporciona aos indivíduos a oportunidade de apresentarem uma queixa alegando violações da HIPAA com HHS (Ventura, 2020).

4.1.3 COPPA

Os tribunais norte-americanos não aplicam proteções de privacidade decorrentes da Quarta, Quinta ou Décima Quarta Emendas, a litígios entre empresas e particulares. Quando os tribunais dos EUA aplicam os estatutos de privacidade, eles adiam para o Congresso e não consideram tipicamente princípios de privacidade constitucional no contexto da interpretação dos estatutos de privacidade oral (Barret, 2019)

Os regulamentos da COPPA são abrangentes, o estatuto aplica-se ao operador de um *website* ou serviço online dirigido a crianças, ou a qualquer operador que tenha conhecimento real de que está a recolher informações pessoais de uma criança. A COPPA aplica-se também a *sites* de terceiros e estabelece um regime de responsabilidade estrita em sites de acolhimento por violações de terceiros. As informações pessoais restritas ao abrigo da COPPA incluem dados de rua, cidade e localização do Estado; endereços de *e-mail*; nomes; identificador persistente que pode ser usado para reconhecer um utilizador ao longo do tempo e em diferentes *sites* de Internet ou serviços *online* (Gupta, 2019).

4.2 Lei de Privacidade e Proteção nos EUA

4.2.1 Lei de Privacidade do Consumidor da Califórnia — CCPA

É o estatuto mais abrangente dos Estados Unidos sobre a lei de privacidade de dados, após alterações previstas; esta nova lei entrou em vigor em janeiro de 2020 e aplicar-se-á a qualquer empresa que cumpra um dos seguintes limiares (Ventura, 2020) (Goldman, 2020):

- Receitas brutas anuais de 25 milhões de dólares;
- Obtém informações pessoais de 50.000 residentes ou mais, agregados familiares ou dispositivos da Califórnia anualmente;
- Cinquenta por cento ou mais receitas anuais a processar informações pessoais dos residentes na Califórnia (Voss & Houser, 2019) (Ventura, 2020).

A motivação por trás da lei é semelhante ao RGPD, ou seja, fornecer proteção legal e soluções para todos os residentes da Califórnia, em que define informações pessoais como qualquer informação que tem a ver com um consumidor particular ou agregado familiar. A expressão "informação pessoal" inclui identificadores únicos, dados de geolocalização, e inferências do comportamento do consumidor (Voss & Houser, 2019).

Baseado no RGPD, a Lei de Proteção do Consumidor da Califórnia, (CCPA) foi assinada em 28 de junho de 2018, e entrou em vigor a 1 de janeiro de 2020; fornece aos residentes da Califórnia uma série de direitos, incluindo o direito de (Ventura, 2020):

- Saber que dados pessoais são recolhidos e como são partilhados;
- Excluir vendas de dados de uma empresa;
- Obrigar uma empresa a apagar dados importantes.

O CCPA fornece aos californianos uma ação privada por violação de dados, uma violação do dever de implementação e manutenção de procedimentos de segurança razoáveis, embora não por violações dos direitos enumerados da Lei.

Os danos causados pela ação privada podem ser severos: o CCPA prevê um maior dano legal entre 100 e 750 dólares por consumidor, por incidente (Ventura, 2020). Ao contrário do RGPD, o CCPA não necessita de uma empresa abrangida para fornecer uma base para a sua recolha de dados ou práticas de processamento. Segundo o CCPA, o Procurador-Geral da Califórnia pode iniciar uma ação civil contra um negócio coberto e recuperar até $2.500 por violação ou $7.500 por violação intencional (Ventura, 2020).

4.2.1.1 As Alterações Legislativas à CCPA

Paul J. Lysobey (2021) defende que os consumidores têm o direito de solicitar às empresas que recolhem ou vendem as suas informações pessoais, as categorias de informações pessoais recolhidas ou vendidas, as fontes usadas, o propósito comercial de recolha dessa informação e as informações específicas recolhidas (Lysobey, 2021). A

Legislatura retirou da definição de informação pessoal, qualquer informação do consumidor que não seja identificada, ou seja, informação relacionada com o consumidor, isto é, informações que não sejam diretamente identificáveis a um consumidor específico e não são informações pessoais desse consumidor. Para ajudar ainda mais a proteger as informações pessoais do consumidor, uma empresa pode exigir que um consumidor que tenha uma conta com a empresa, apresente todos os pedidos de informação através dessa conta.

As empresas continuam a ser responsáveis perante os consumidores, pela violação de dados; no entanto, essa responsabilidade baseia-se agora no acesso não autorizado, roubo ou divulgação de informações pessoais não encriptadas, em vez de informações pessoais não encriptadas. Com esta mudança, a Legislatura dificultou manter uma reivindicação sob o CCPA para uma violação de dados.

Segundo Mark Peasley (2019) o congresso norte-americano introduziu vários projetos de lei que tentaram melhorar as leis atuais de proteção de dados dos EUA. Essas contas incluem a Lei de Proteção à Privacidade dos Consumidores de 2017, a Lei de Segurança de Dados e Notificação de Violação, a Lei do Escudo Cibernético de 2017 e a Lei de Proteção de Dados do Consumidor. Com esses projetos a lei trouxe também novas restrições no que toca a privacidade de dados.

4.2.1.2 Novas Restrições na Recolha de Dados e na Garantia de Dados Corretos

A Lei de Proteção da Privacidade dos Consumidores de 2017 teria limitado a recolha de dados de uma forma muito parecida com o RGPD. Se fosse aprovada, a Lei teria exigido que todas as entidades abrangidas criassem um plano para minimizar a quantidade de dados pessoais armazenados pela entidade e minimizar o tempo de armazenamento dos dados (Peasley, 2019).

4.2.1.3 Novas Restrições a Processamento de Dados

A Lei de Segurança de Dados e Notificação de Violação de 2017 teria exigido que qualquer entidade abrangida que processasse os dados tivessem uma política que indicasse como os dados serão mantidos ou utilizados. Estas políticas poderiam ter levado os EUA a igualar o RGPD (Peasley, 2019).

4.2.1.4 Novo Regulamento Relativo à Violação e Prevenção de Acesso não Autorizado

A Lei de Proteção da Privacidade dos Consumidores de 2017 teria exigido que as entidades abrangidas determinassem vulnerabilidades e ameaças, que pudessem levar ao acesso, transferência, destruição ou utilização não autorizada de informações pessoais. A entidade teria então de determinar os potenciais danos que podem resultar das vulnerabilidades e ameaças e determinar o quão suficientes são as suas precauções de segurança (Peasley, 2019).

4.2.1.5 Os Regulamentos Finais

Os regulamentos finais identificam três avisos exigidos pelo CCPA (Lysobey, 2021):

- Avisos exigidos a uma empresa que recolha informações pessoais;
- Avisos de exclusão exigidos a uma empresa que venda informações pessoais;
- Avisos necessários de uma empresa que oferece um incentivo financeiro ou diferença de preço, ou serviço.

Segundo Paul J. Lysobey (2021) todas as empresas que recolhem informações pessoais dos consumidores, são obrigadas a fornecer um aviso, atempadamente, no ponto de recolha, sobre as categorias de informações pessoais a recolher e uma explicação do motivo pelo qual a informação está a ser recolhida. Uma empresa não pode recolher outras categorias de informação fora das categorias descritas no aviso.

O aviso de cobrança deve incluir (Lysobey, 2021):

- Uma lista das categorias de informações pessoais a recolher;
- O objetivo comercial ou não comercial para o qual as informações serão utilizadas;
- Uma ligação à política de privacidade da empresa.

Os regulamentos estabelecem que o aviso de incentivo financeiro deve incluir as seguintes informações (Lysobey, 2021):

- Um resumo do incentivo financeiro ou do preço, ou diferença de serviços oferecidos;
- Uma descrição das condições materiais do incentivo;
- A forma como um consumidor pode optar pelo incentivo;
- Uma declaração de que o consumidor pode retirar-se do incentivo financeiro a qualquer momento e como exercer esse direito;
- Uma explicação de como o incentivo está razoavelmente relacionado ao valor dos dados do consumidor, que deve incluir uma estimativa de boa-fé do valor dos dados do consumidor, constituindo uma base para o incentivo e uma descrição de como a empresa calculou o valor dos dados do consumidor.

Os regulamentos finais, exigem que todas as empresas sujeitas ao CCPA forneçam aos consumidores uma política de privacidade; o objetivo da política de privacidade é fornecer aos consumidores uma descrição das práticas de uma empresa, tanto *online* como *offline*, no que diz respeito à recolha, utilização, divulgação e venda de informações pessoais e dos direitos dos consumidores relativamente às suas informações pessoais (Lysobey, 2021).

4.2.1.6 Direitos dos Consumidores Criados pela Lei

Fundamentalmente, o CCPA destina-se a promover o direito pessoal à privacidade ao abrigo da Constituição da Califórnia. Para isso, o CCPA fornece vários meios práticos para os residentes da Califórnia afirmarem um maior controlo sobre as informações pessoais recolhidas. Assim, segundo a lei, os consumidores da Califórnia têm os seguintes direitos adicionais (Goldman, 2020):

4.2.1.6.1 Direito de Saber e de Portabilidade de Dados

O CCPA permite que os consumidores conheçam as práticas de dados das empresas (*online* e *offline*), sendo as empresas obrigadas a fazer divulgações sobre as suas práticas genéricas de recolha (1798.100) e as suas vendas ou transferências de dados (1798.115).

A pedido, as empresas devem também divulgar as categorias específicas de informação pessoal que recolheram junto do consumidor e as peças específicas de informação pessoal, que recolheram sobre esse consumidor, num formato portátil (1798.110); o CCPA tem requisitos detalhados para as políticas de privacidade (especialmente 1798.130(a)(5), e os regulamentos adicionam muitos mais requisitos. Por exemplo, as páginas web que contenham as divulgações legais, devem estar em conformidade com as normas de acessibilidade W3C e estes direitos criam caminhos para os malfeitores obterem ilegitimamente dados valiosos do consumidor (Goldman, 2020).

4.2.1.6.2 Direito de Eliminar (1798.105)

A pedido de um consumidor, uma empresa deve apagar quaisquer informações pessoais sobre o consumidor. As empresas podem recusar os pedidos quando (Goldman, 2020):

- Concluírem a transação ou uma transação esteja razoavelmente prevista;
- Encontrarem, prevenirem ou processarem violações de segurança, ou atividades ilegais;
- Identificarem e repararem erros que comprometam a intenção da existente funcionalidade;
- Exercerem a liberdade de expressão da empresa ou de um terceiro, ou exercerem outro direito previsto na lei;
- Cumprirem com a ECPA da Califórnia;
- Envolverem-se em determinados tipos de investigação em casos limitados;
- Permitirem usos exclusivamente internos razoavelmente, alinhados com as expectativas do consumidor, com base na relação do consumidor com o negócio;
- Cumprirem uma obrigação legal;

- Utilizarem internamente as informações pessoais do consumidor, de forma lícita compatível com o contexto em que o consumidor forneceu as informações.

4.2.1.6.3 Direito de Dizer "não" às Vendas de Dados

Os consumidores podem controlar a capacidade das empresas de venderem os seus dados (Goldman, 2020):

- **Excluir Vendas de Dados (1798.120 (a))** — os consumidores podem optar por não vender as suas informações pessoais, e a empresa não pode pedir-lhes que reconsiderem durante pelo menos 12 meses (1798.135 (a) (5)) com exceções limitadas especificadas nos regulamentos.

- **Opte por Vendas de Dados Relacionadas com Menores (1798.120(d))** — uma empresa que conheça (ou "desrespeita deliberadamente" a idade do consumidor) informações pessoais relacionadas com consumidores com menos de 16 anos não pode vender a informação pessoal a menos que o consumidor (dos 13 aos 15 anos) ou o progenitor/ tutor (menores de 13 anos) concorde.

- **Excluir Revenda de Dados a um Terceiro (1798.115 (d))** — um terceiro não deve vender informações pessoais sobre um consumidor que tenha sido vendido a terceiros por uma empresa, a menos que o consumidor tenha recebido um aviso explícito e tenha a oportunidade de exercer o direito de não optar.

- **Especificações para divulgação de exclusão de vendas de dados** (1798.135) — se uma empresa vender informações pessoais, deve então fornecer um *link* claro e visível na página inicial do sítio web, intitulada: não vender as minhas informações pessoais.

4.2.1.6.4 Disposições Relativas à não Discriminação (1798.125)

Uma empresa não discrimina um consumidor porque o consumidor exerceu qualquer um dos direitos do consumidor ao abrigo deste título, embora uma empresa possa cobrar

a um consumidor um preço ou taxa diferente, ou fornecer um nível, ou qualidade diferente de bens, ou serviços a esse mesmo consumidor.

As empresas podem oferecer incentivos financeiros (definidos como um programa, benefício ou outra oferta, incluindo pagamentos aos consumidores, relacionados com a cobrança, retenção ou venda de informações pessoais) para compensar a cobrança, venda ou eliminação de dados, mas não se os incentivos financeiros forem injustos, irrazoáveis (Goldman, 2020).

4.2.1.6.5 Direito de Ação Privado para Violações de Dados

A lei cria uma causa privada de ação quando informações pessoais não encriptadas estão sujeitas a um acesso não autorizado, roubo ou divulgação em consequência da violação do dever de aplicação e manutenção de procedimentos e práticas de segurança razoáveis adequados à natureza das informações, para proteger as informações pessoais (1798.150). Em caso de violação de dados, os consumidores podem obter um valor entre os 100 a $750 por incidente e por consumidor; de modo a dar seguimento ao processo judicial, o consumidor tem que dar à empresa 30 dias para resolver a questão de segurança. Se a empresa conseguir resolver o problema, então o contexto de violação ou falha de segurança fica resolvido e o valor a receber fica indisponível (Goldman, 2020).

4.2.2 Lei de Privacidade de Washington — WPA

Em 2021, os senadores do Estado de Washington propuseram um projeto de lei intitulado WPA, a terceira tentativa do Estado de uma lei de privacidade de dados; o WPA fornece aos residentes de Washington muitos dos mesmos direitos estabelecidos ao abrigo do CCPA (Ventura, 2020).

Ao abrigo da lei, os residentes de Washington têm direito a:

- Categorias de acesso de informações processadas sobre eles;
- Imprecisões corretas;
- Supressão do pedido;
- Receber as suas informações pessoais recolhidas;

- Excluir o tratamento de informação para, entre outros fins, publicidade direcionada e vendas de terceiros (Ventura, 2020).

No entanto, em comparação com o CCPA, o WPA reduz a fronteira das empresas que se enquadram na alçada do estatuto. A lei aplica-se às empresas que:

- Processam informações pessoais de mais de 100.000 residentes em Washington,

- Obtenham mais de 25% das suas receitas anuais, com a venda de informações pessoais e processem informações pessoais de mais de 25.000 residentes em Washington.

O WPA limita a capacidade dos residentes de Washington de recuperarem por violações; ao contrário do CCPA, o WPA não fornece uma ação privada para os residentes de Washington. Apenas o Procurador-Geral de Washington pode impor violações do WPA e recuperar até $7.500 por violação. Os críticos do WPA argumentam que o projeto de lei que a Amazon e a Microsoft apoiam é centrado nas empresas com uma linguagem vaga, uma lista de isenções e uma provisão que proíbe explicitamente as pessoas de responsabilizarem as empresas quando violam os direitos de privacidade digital das pessoas. Entretanto, os apoiantes argumentam que o projeto de lei oferece proteções de privacidade claras, acessíveis e exequíveis e é uma das mais fortes a nível global com um quadro de privacidade robusto (Ventura, 2020).

4.2.3 Lei de Privacidade de Nova Iorque — NYPA

Em janeiro de 2021, os senadores do estado de Nova Iorque reintroduziram a anterior sessão legislativa da NYPA. A NYPA está atualmente na Comissão dos Assuntos do Consumidor e da Proteção como Lei de Assembleia (Ventura, 2020).

De âmbito mais alargado do que o CCPA e o WPA, a NYPA não define o termo negócio, e carece de um limiar de receitas ou de consumo superior ao que exporia as empresas à responsabilidade.

Ao contrário do RGPD, CCPA e WPA, a NYPA contém uma cláusula que estabelece o dever de cuidado, que as empresas devem aos consumidores sobre a manutenção dos seus dados (Ventura, 2020). A cláusula estabelece que as empresas devem agir no melhor

interesse do consumidor, independentemente dos interesses da entidade, do controlador ou do corretor de dados. Não só as empresas terão de enfrentar um nível de cuidado mais elevado, como também terão de determinar, potencialmente, os melhores interesses de cada consumidor (Ventura, 2020).

A NYPA também fornece amplos mecanismos de aplicação da lei que podem levar a uma inundação de processos nos tribunais estaduais. Embora a NYPA defina consumidores como residentes em Nova Iorque, não define pessoa, expandindo ainda mais o universo de potenciais queixosos. E a NYPA expõe as empresas a uma enorme responsabilidade (Ventura, 2020).

4.2.4 Lei de Proteção de Dados dos Consumidores Virgínia CDPA

A Virgínia tornou-se o segundo estado depois de a Califórnia a aprovar uma lei de privacidade abrangente, quando o governador Ralph Northam assinou a Lei de Proteção de Dados do Consumidor (CDPA), para promulgar uma lei geral abrangente de privacidade. O CDPA partilha características comuns com a Lei de Privacidade da Califórnia e contas de privacidade do Estado, mas também contém os seus requisitos únicos próprios. Como resultado destes requisitos únicos, as empresas sujeitas ao CDPA, que está prestes a entrar em vigor a 1 de janeiro de 2023, terão de tomar medidas específicas, para garantir que o seu tratamento de dados o cumpra (Simmons, 2021).

4.2.4.1 Área de Atuação

O CDPA aplica-se às empresas que operam na Virgínia ou produção de produtos, ou serviços comercializados para os residentes da Virgínia, que se encontram com um dos seguintes limiares relativos a atividades de dados (Simmons, 2021):

- Controlar ou processar dados pessoais de 100.000, ou mais consumidores da Virgínia num ano civil;
- Controlar ou processar dados pessoais de pelo menos 25.000 consumidores da Virgínia e obter mais de 50% das receitas brutas da venda de dados pessoais;
- Instituições financeiras sujeitas a disposições pertinentes da Lei *Gramm-Leach-Bliley* que gere a privacidade e a segurança dos consumidores;

- As entidades de cuidados de saúde ou os seus fornecedores designados por associados empresariais regidos pelas regras de privacidade, segurança e incumprimento das regras de portabilidade e responsabilização dos seguros de saúde (HIPAA), leis e regulamentos.

4.2.4.2 Direito dos Consumidores

À semelhança de outras leis de privacidade abrangentes, como a Lei de Privacidade da Califórnia e o RGPD da UE, o CDPA fornece aos consumidores inúmeros direitos aos seus dados pessoais. Os consumidores podem exercer estes direitos contra empresas que atuam como controladoras e semelhante ao RGPD, uma empresa atua como controlador sob o CDPA pode determinar a finalidade e meios de tratamento dos dados pessoais (Simmons, 2021).

4.2.4.3 Confirmação do Processamento de Dados

A empresa deve confirmar ao consumidor se o negócio processa dados pessoais sobre esse consumidor (Simmons, 2021).

4.2.4.4 Acesso

A empresa deve facultar ao consumidor o acesso aos seus dados pessoais, não definindo o CDPA expressamente o que o acesso requer. No entanto, segundo a interpretação do direito de acesso ao abrigo de outras leis de privacidade, as empresas devem provavelmente estar preparadas, no mínimo, para fornecer aos consumidores solicitados a possibilidade de visualizarem quaisquer dados pessoais que a empresa mantenha sobre esse consumidor (Simmons, 2021).

4.2.4.5 Correção

A empresa deve corrigir dados pessoais imprecisos sobre o consumidor, tendo em conta a natureza dos dados pessoais e as finalidades do tratamento dos dados pessoais do consumidor (Simmons, 2021).

4.2.4.6 Eliminação.

A empresa é obrigada a apagar os dados pessoais fornecidos ou obtidos sobre esse consumidor. Este direito de supressão parece mais amplo do que o mesmo direito sob a Lei de Privacidade da Califórnia, exige que as empresas apaguem informações pessoais do consumidor final ou titulares dos dados que elas (empresas) tenham recolhido (Simmons, 2021).

4.2.4.7 Portabilidade

A empresa deve fornecer ao consumidor os seus dados previamente fornecidos à empresa, num formato portátil e na medida tecnicamente viável, facilmente utilizável, que permita transferências de dados para outros controladores de dados (Simmons, 2021).

4.2.4.8 Exclusão

O CDPA da Virgínia fornece um conjunto de direitos de exclusão da publicidade direcionada, venda de dados e certos perfis que podem resultar em efeitos legalmente significativos (Simmons, 2021).

4.2.4.9 Segurança dos Dados

O CDPA exige que os controladores de dados estabeleçam e mantenham práticas razoáveis de segurança administrativa, técnica e física, para proteger a confidencialidade, integridade e acessibilidade dos dados pessoais. Estas normas não são definidas em detalhe e provavelmente apresentam uma margem significativa para interpretação pelo Procurador-Geral da Virgínia em execução, incluindo a resposta a violações de dados (Simmons, 2021).

4.2.4.10 Aviso

O aviso adequado ao consumidor é fundamental para apoiar a atividade de processamento de dados de uma empresa ao abrigo do CDPA; à semelhança de outras leis e propostas abrangentes de privacidade, o CDPA reflete um princípio de cobrança limitada. As empresas devem assegurar que os seus avisos reflitam todas as atividades relevantes de recolha e utilização de dados (Simmons, 2021).

4.2.4.11 Processar Dados Sensíveis

O CDPA proíbe qualquer tratamento de dados sensíveis por um controlador de dados sem o consentimento do consumidor. Tanto os dados sensíveis como os consentimentos são definidos no CDPA (Simmons, 2021):

- Dados sensíveis incluem dados pessoais que revelem "origem racial ou étnica, crenças religiosas, diagnóstico de saúde mental ou física, orientação sexual ou cidadania, ou estatuto de imigração; dados genéticos ou biométricos utilizados para identificar uma pessoa singular; dados pessoais recolhidos de um indivíduo conhecido por ser uma criança com menos de 13 anos; e informações precisas de geolocalização que identifiquem a localização de uma pessoa num raio de 1.750 pés.

- O consentimento requer um ato afirmativo claro e deve ser livre, específico, informado e inequívoco. O consentimento implícito não satisfaz esta norma.

As leis dos Estados Unidos em matéria de proteção de dados, são atualmente uma recolha de retalhos de legislação que se centram, principalmente, em determinadas áreas do comércio e certos tipos de negócio. Para além dessas áreas e das empresas, a proteção de dados tem sido uma questão prática para o Congresso, embora alguns regulamentos recentemente propostos demonstrem que alguns, no Congresso podem estar dispostos a tomar uma abordagem mais dura em matéria de proteção de dados (Peasley, 2019).

5 Privacidade de Dados na EU vs EUA

Catherine Barrett (2019) defende que, as diferenças culturais entre os EUA e a EU, em matéria de direitos de privacidade e proteção de dados, significam que as empresas americanas podem ter dificuldade em compreender e implementar o RGPD. O facto de os cidadãos americanos não terem direitos e proteções gerais de privacidade de dados consagrados na Constituição ou estatuto federal, resulta em que as empresas, pelo menos inicialmente, tratam os dados de forma diferente nos EUA em comparação com a UE (Barrett, 2019).

Chetan Gupta (2019) afirma haver uma diferença entre as leis: é que a maioria das leis de privacidade dos EUA, incluindo o CCPA, apenas protegem a privacidade dos residentes, enquanto o RGPD e a Lei de Proteção de Dados Pessoais na EU, regulam qualquer tratamento de dados pessoais em territórios locais, incluindo dados pessoais relativos a pessoas residentes noutros países (Gupta, 2019).

Segundo o estudo desenvolvido por Mark Peasley (2019), existe uma grande diferença, quando se abordam temas sobre privacidade de dados entre UE e EUA; ele centrou o seu estudo nos pontos seguintes, focando-se nas leis que se aplicam na UE e, de uma forma generalizada, sobre as leis aplicadas nos EUA; estes são os objetos de comparação entre os dois continentes (Peasley, 2019):

- Restrições à recolha de dados e à garantia de dados corretos;
- Restrições no tratamento de dados;
- Restrições à transferência de dados;
- Violação e prevenção de acessos não autorizados;
- Notificação e atenuação de prejuízos na sequência de uma violação de dados;
- Supervisão e responsabilidade das entidades abrangidas.

5.1 Restrições à Recolha de Dados e à Garantia de Dados Corretos

5.1.1 UE — RGPD

O RGPD é uma legislação muito mais abrangente do que a homóloga dos norte-americanos; começa a regular a proteção de dados antes de o titular dos dados fornecer as suas informações à entidade abrangida, e continua a sua regulação através da fase de processamento e armazenamento, até à eliminação das informações protegidas (Peasley, 2019).

Os dados são recolhidos apenas para fins explícitos e legítimos, e devem limitar-se ao necessário para o efeito; além disto, o RGPD exige que cada titular de dados dê o seu consentimento livremente, para armazenar os seus dados pessoais e revogar o consentimento para o armazenamento ou tratamento das suas informações pessoais (Peasley, 2019). O RGPD impõe ainda restrições adicionais à recolha de determinados tipos de dados, incluindo origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, ou adesão sindical e dados relativos à saúde ou orientação sexual (Peasley, 2019).

5.1.2 EUA

Nos EUA, a lei atual limita a recolha de dados, tal como a lei de proteção de dados em geral, e é uma tentativa de regular a recolha de dados em certas áreas. Por exemplo, para informações médicas, a HIPAA exige que seja dado ao titular dos dados a oportunidade de se opor, embora o silêncio seja igual a consentimento, à entidade que armazena o nome do titular dos dados, a localização, etc. HIPAA falha em permitir que determinadas informações sejam armazenadas, embora exista um pretexto de exigir consentimento (Peasley, 2019).

A FCRA impõe aos fornecedores de dados o dever de fornecer informações precisas, bem como o dever de corrigir erros; se qualquer informação que o fornecedor está a fornecer a uma agência de crédito for negativa, o fornecido deve notificar o titular dos dados das informações negativas e conceder-lhe a oportunidade de corrigir os dados (Peasley, 2019).

5.2 Restrições no Processamento/Tratamento de Dados

5.2.1 UE — RGPD

O tratamento dos dados, refere-se à forma como os dados recolhidos devem ser utilizados uma vez recolhidos; o RGPD define um processador separadamente como uma pessoa singular ou legal, autoridade pública, agência ou outro organismo que processa dados pessoais, em nome do responsável pelo tratamento. Um processador pode também ser a mesma entidade que recolhe os dados. Se as entidades (empresas que tratam ou processam os dados) forem as mesmas, o processador limita-se a utilizar os dados apenas pelas razões especificadas no contrato entre a entidade de recolha e o processador especificado. O RGPD define explicitamente o tratamento, como uma fase separada do ciclo de proteção de dados e aborda-o individualmente, exigindo o consentimento de um titular dos dados para que os seus dados sejam tratados. O titular dos dados deve ser informado sobre a finalidade da recolha, de como serão utilizados e tratados antes da recolha, e o consentimento do titular dos dados deve ser dado livremente, específico, informado e inequívoco (Peasley, 2019).

5.2.2 EUA

Nos Estados Unidos da América não existem limites específicos para o processamento ao abrigo da lei atual, e o tratamento de dados parece ser uma área maioritariamente autorregulada; a maioria das pessoas que têm a opção de escolher se devem ou não fornecer as suas informações, têm apenas uma ideia de como os dados serão utilizados. As limitações de processamento seriam mais úteis em circunstâncias em que o tratamento não seja imediatamente óbvio para o titular dos dados, como por exemplo, para posterior comercialização e venda de informação a outras entidades (Peasley, 2019).

5.3 Restrições à Transferência de Dados

5.3.1 UE — RGPD

A legislação em matéria de proteção de dados deve equilibrar as necessidades do comércio, que beneficia de transferências abertas de dados, com as necessidades de privacidade e segurança do titular dos dados, que beneficiam de transferências mínimas

de dados. O RGPD centra-se principalmente na transferência de informação para fora da União Europeia, para entidades não abrangidas.

5.3.2 EUA

Os regulamentos dos Estados Unidos também colocam uma ênfase significativa em limitar as transferências de informação, em vários regulamentos diferentes; a FCRA autoriza transferências de informação pessoal em diversas situações, por entidades abrangidas, embora essas situações sejam limitadas. Para proteger a pessoa em causa no seu emprego, uma entidade abrangida só pode fornecer um relatório de crédito a um empregador se o empregador certificar que cumpriu a FCRA, se tiver fornecido ao titular dos dados um resumo dos seus direitos, tendo o titular dos dados sido notificado de que pode ser obtido um relatório e consentido a divulgação ao empregador por escrito (Peasley, 2019). Tanto no direito europeu como nos Estados Unidos, grande parte do foco nas regras de proteção de dados diz respeito à transferência de dados. As restrições abrangentes às transferências de dados correriam o risco de sufocar o comércio, enquanto o subsídio completo das transferências de dados sem regulamentação dificultaria o controlo de quem tinha acesso a informações pessoais e como essa informação é distribuída a outras entidades. No entanto, o HIPAA é muito parecido com o RGPD, em que apenas protege informações identificáveis.

Enquanto as informações transferidas não puderem identificar um titular individual de dados, a entidade abrangida não é obrigada a cumprir os requisitos de transferência acima indicados, mesmo que as informações não identificantes sejam criadas a partir de informações pessoalmente identificáveis (Peasley, 2019).

5.4 Violação e Prevenção de Acessos Não Autorizados

5.4.1 UE — RGPD

O primeiro passo para impedir o acesso não autorizado a informações pessoais, é determinar o risco de tentativas de acesso e quais os riscos que o acesso não autorizado representaria a um titular de dados. Ao abrigo do RGPD, a avaliação do impacto da proteção de dados é particularmente necessária, quando o processamento automatizado possa produzir um efeito legal sobre uma pessoa, o tratamento é em grande escala e

envolve os tipos especiais de informação acima descritos. A avaliação completa do impacto da proteção de dados deve conter o seguinte (Peasley, 2019):

- Uma descrição das operações e finalidades de tratamento;
- Uma avaliação da proporcionalidade e da necessidade em relação aos fins de transformação;
- Uma avaliação dos riscos para os direitos e liberdades da pessoa em causa, incluindo o direito à privacidade;
- Medidas previstas para fazer face aos riscos identificados.

O segundo passo para impedir o acesso não autorizado, é tomar medidas para mitigar os riscos avaliados, como obrigar as entidades responsáveis a implementarem medidas adequadas para garantir a segurança adequada ao risco, incluindo o pseudónimo ou a encriptação dos dados; meios para garantir a continuação da confidencialidade, integridade, disponibilidade e resiliência de sistemas e serviços de processamento (Peasley, 2019).

5.4.2 EUA

As leis de proteção de dados dos Estados Unidos, tomam uma abordagem mais generalizada às violações; a HIPAA é a regulamentação solitária dos Estados Unidos, que exige que as entidades abrangidas realizem uma avaliação dos riscos para a confidencialidade, integridade e disponibilidade de informações de saúde protegidas.

As entidades abrangidas devem então agir sobre essa avaliação de risco, implementando medidas de segurança para reduzir os riscos a um nível razoável, sancionando os funcionários que não satisfaçam os requisitos da política de segurança e implementando formas de rever a atividade do sistema de armazenamento de dados (Peasley, 2019).

A FCRA exige que as entidades abrangidas utilizem procedimentos razoáveis, para evitar violações da FCRA e limitar as transferências não autorizadas, apenas para os fins aprovados pela FCRA. A FCRA prevê ainda que as agências bancárias federais, a Administração Nacional da União de Crédito, a Comissão Federal do Comércio, a

Comissão de Negociação de Futuros de Mercadorias e a Comissão de Mercado de Valores Mobiliários estabelecerão orientações para as instituições financeiras e credores por roubo de identidade, prescreverão regulamentos para identificar riscos para os sujeitos, dados e regulamentos que diminuam o risco de roubo de identidade ou de encargos fraudulentos (Peasley, 2019).

5.5 UE – RGPD vs EUA – CCPA

De acordo com a afirmação de Catherine Barrett (2019), há diferenças no ponto de vista dos direitos de privacidade e as proteções de dados nos EUA e na UE. Os europeus operam numa perspetiva de que os clientes possuem os seus dados, enquanto as empresas norte-americanas vêem-se como proprietárias dos dados porque são ou os empregadores ou os que gastaram milhões (ou milhares de milhões) para recolher e analisar esses dados. A privacidade e proteção de dados são dois direitos consagrados nos Tratados da UE e na Carta dos Direitos Fundamentais da UE. A UE elevou a privacidade dos dados para o domínio dos direitos individuais e protegeu esses direitos através do Regulamento Geral de Proteção de Dados. Ainda com a afirmação de Catherine Barrett (2019), ao contrário da UE, nos EUA não há direito individual à privacidade dos dados e, ou a proteção de dados consagrados na Constituição dos EUA.

A Quarta Emenda, não prevê um direito à privacidade constitucional; em vez disso, protege a privacidade individual contra certos tipos de intrusões governamentais, por outras palavras, a Quarta Emenda protege as pessoas de buscas e apreensões irrazoáveis por parte do governo, mas não garante um direito geral à privacidade (Barrett, 2019). As tabelas 1 e 2 foram derivadas a partir da fonte obtida no trabalho de Jehl & Friel (2018).

Os Direitos	**EUA - CCPA**	**UE - RGPD**	**Comparação**
Portabilidade dos Dados	Em resposta a um pedido de divulgação, uma empresa deve fornecer informações pessoais num formato facilmente utilizável para permitir que um consumidor transmita a informação de uma entidade para outra entidade, sem entraves.	O RGPD inclui um novo direito à portabilidade dos dados, para receber uma cópia dos dados pessoais num formato estruturado, comummente utilizado e legível por máquina e, também transmitir os dados pessoais a outro controlador de dados (incluindo diretamente por outro controlador de dados, sempre que possível).	Direitos semelhantes, o RGPD fornece um direito específico de solicitar a um controlador de dados a transferência dos seus dados pessoais, para outro responsável pelos dados.

Eliminação (a ser esquecido)	O consumidor tem o direito de excluir informações pessoais que uma empresa recolheu, sob reserva de determinadas exceções. A empresa também deve instruir os seus prestadores de serviços a apagar os dados.	Os titulares dos dados, têm o direito de solicitar o apagamento dos dados pessoais em seis circunstâncias (o direito a ser esquecido). Os controladores de dados, também devem tomar medidas razoáveis para informar quaisquer outros controladores de dados, que também processem os dados.	Direitos de eliminação de dados semelhantes. O direito do RGPD só se aplica se o pedido satisfaça uma das seis condições específicas enquanto o direito CCPA é amplo. No entanto, o CCPA também permite que as empresas recusem o pedido por motivos muito mais amplos do que o RGPD. A obrigação do RGPD de informar os destinatários dos dados a jusante do pedido de eliminação da pessoa é também mais ampla
Retificação	Nenhum	O RGPD concede aos titulares dos dados o direito de: corrigir dados pessoais quando estiverem incompletos.	Substancialmente diferente.
Restringir o Processamento	Nenhum, além do direito de excluir a venda de informações pessoais.	Direito de restringir o tratamento de dados pessoais, sob determinadas circunstâncias.	Substancialmente diferente.
Objeto ao processamento	Nenhum, além do direito de excluir a venda de informações pessoais.	Direito de oposição ao processamento para fins de perfis, marketing direto e estatística, científica ou histórica.	Substancialmente diferente.
Excluir para venda de informações pessoais	As empresas devem permitir e cumprir o pedido do consumidor de excluir a venda de informações pessoais a terceiros, sob reserva de determinadas defesas. Deve incluir um *link* "Não vender as minhas informações pessoais" numa localização clara e visível numa página inicial do site.	O RGPD não inclui um direito específico de excluir as vendas de dados pessoais. No entanto, o RGPD contém outros direitos que um titular dos dados pode utilizar para obter um resultado semelhante, em determinadas circunstâncias. Isto permite que os titulares dos dados optem por excluir as vendas de terceiros, que suportem fins de marketing ou dependam do consentimento, para a sua base de processamento legal.	Substancialmente diferente.

Tabela 1 Resultado da Comparação entre UE vs EUA P1, fonte (Jehl & Friel, 2018)

	EUA - CCPA	**UE - RGPD**	**Comparação**
Quem é regulado?	Qualquer negócio na Califórnia, que atenda a um dos seguintes: tem uma receita bruta superior a $25 milhões. Anualmente compra, recebe, vende ou partilha a informação pessoal de mais de 50.000 consumidores, famílias	Processador ou Controlador de dados: na UE processam dados pessoais no contexto de atividades do estabelecimento da EU, independentemente de o processamento de dados se realizar na UE. Processar dados pessoais de um	O alcance territorial do RGPD é muito mais amplo. Substancialmente diferente.

	ou dispositivos para fins comerciais. Obtém 50% ou mais das suas receitas anuais com a venda de informações pessoais dos consumidores. A lei aplica-se também a qualquer entidade que controla ou é controlada por uma empresa abrangida e partilha a marca comum com um negócio coberto, como um nome partilhado, marca de serviço ou marca registada.	indivíduo fora da UE, diz respeito à oferta de bens ou serviços na UE.	
Quem está protegido?	Consumidores, definidos como residentes da Califórnia que são: estão na Califórnia para outros fins que não seja um propósito temporário ou transitório. Com residência na Califórnia, mas estão atualmente fora do Estado para um propósito temporário ou transitório. Os consumidores incluem: clientes de bens e serviços domésticos. Os empregados. Transações entre negócios.	Sujeitos de dados, definidos como pessoas identificadas ou identificáveis a que os dados pessoais se relacionam.	Substancialmente diferente na abordagem, mas igualmente ampla em vigor. Ambas as leis se centram na informação relacionada com uma pessoa singular identificável, no entanto as definições diferem. Ambos têm potenciais efeitos extraterritoriais que as empresas localizadas fora da jurisdição devem considerar.
Que informação é protegida?	As informações pessoais que se identifiquem, se relacionem, sejam capazes de estar associadas, ou possam razoavelmente estar ligadas, direta ou indiretamente, a um determinado consumidor ou agregado familiar. A definição legal inclui uma lista de categorias específicas de informações pessoais. O CCPA exclui do seu âmbito de cobertura determinadas informações pessoais abrangidas por outras legislações, específicas do sector.	Os dados pessoais são qualquer informação relativa a um titular de dados identificado ou identificável. O RGPD proíbe o tratamento de categorias especiais definidas de dados pessoais, a menos que seja aplicável uma justificação legal para o tratamento.	Substancialmente similar. No entanto, a definição CCPA também inclui informações ligadas ao nível do agregado familiar ou do dispositivo.

Tabela 2 Resultado da Comparação entre UE vs EUA P2, fonte (Jehl & Friel, 2018)

6 Privacidade de Dados (UE) — Computação em Nuvem

Para estar em conformidade com o RGPD, os serviços em nuvem que gerem regularmente dados, devem ser concebidos para responder a questões de privacidade (privacidade por *design*), permitir o processamento apenas dos dados que são absolutamente necessários para operações do sistema, e limitar o acesso aos dados a apenas pessoas envolvidas no processamento. Foi necessário implementar políticas e ferramentas, para dar aos titulares de dados o direito de transferir os seus dados pessoais para outros fornecedores, e de apagar os seus dados quando já não precisam de ser tratados (Russo et al., 2018).

O PaaS oferece um ambiente de desenvolvimento e implementação na nuvem, representando a camada do sistema operativo. Como exemplo refere-se o Google App Engine e Microsoft Azure; em termos de acesso aos dados, a aplicação está sob o controlo do cliente. No entanto, o cliente não tem controlo direto sobre o ambiente de execução e os mecanismos de registo e encriptação podem ser implementados na plataforma, para que os fornecedores possam recolher e armazenar os dados, para serem utilizados pelo cliente com diferentes finalidades, como verificações de segurança (Russo et al., 2018).

Em termos de processamento de dados, as tecnologias SaaS e IaaS estão em extremos da mesma escala, pelo que os seus fornecedores têm responsabilidades e funções diferentes. Um fornecedor IaaS, normalmente, oferece um serviço de aplicação de *software* que se destina especificamente a processar dados pessoais. Um fornecedor SaaS pode exercer uma vasta gama de controlos em relação aos dados tratados, utilizando o seu SaaS (Russo et al., 2018).

Dado que o RGPD abrange todas as entidades que armazenam, processam ou transferem dados na União Europeia, bem como as que armazenam, processam ou transferem dados relativos a pessoas que residem na União Europeia ou onde se aplicam as leis dos Estados Membros da União Europeia, todas as entidades abrangidas são mantidas nas mesmas normas (Peasley, 2019).

O RGPD garante que qualquer entidade abrangida que receba uma transferência de informações pessoais, deverá possuir o mesmo nível de segurança e seguir os mesmos regulamentos que a entidade que transfere as informações pessoais; assim, estabelece duas formas de uma entidade não abrangida receber uma transferência de informações pessoais de uma entidade abrangida: por decisão de adequação ou por cumprimento das salvaguardas adequadas (Peasley, 2019).

6.1 Fornecedor de Serviços na Nuvem no RGPD

Segundo a afirmação de Barbara Russo et al. (2018), foi introduzido um elemento importante pelo RGPD, que tem um impacto significativo nos serviços e na nova responsabilidade atribuída ao processador.

O papel de um fornecedor em serviços na nuvem, nas recentes diretivas europeias em que os CSPs são operadores, que disponibilizam as suas infraestruturas para o tratamento de dados, por outras palavras, o fornecedor de mapeamento como processador e não como controlador, deriva da natureza da atividade realizada pelo fornecedor para o armazenamento em nuvem (Russo, et al., 2018).

Segundo Axel Bussche (2017), sobre o tratamento de dados pessoais através dos sistemas geridos pelos fornecedores de nuvem, as entidades determinam as finalidades e meios de processamento, mas as operações são realizadas pelos prestadores de serviços. Assim, os clientes dos serviços na nuvem qualificam-se como controladores e prestadores de serviços na nuvem como processadores no âmbito do RGPD. Quanto mais influência o prestador de serviços em nuvem tem nos meios e propósitos de processamento, maior é a probabilidade de se qualificar como controlador no âmbito do RGPD. Por exemplo, quando o fornecedor de serviços na nuvem processa dados pessoais para os seus próprios fins, pode ser qualificado como controlador (Bussche, 2017).

6.1.1 CSP como Processador

O fornecedor oferece sistemas de retenção e armazenamento de dados, em nome do cliente, e disponibiliza-os imediatamente a qualquer pessoa com acesso autorizado, a qualquer momento e de qualquer parte do mundo, através de uma ligação à Internet. Em alguns casos, um CSP que oferece serviços de processamento de dados pessoais diretamente a titular de dados como *Facebook* ou *Dropbox* é considerado um controlador

de dados, visto que determina a finalidade e os meios para esses serviços de processamento. As novas formas de dados geradas pelas modernas infraestruturas e plataformas em nuvem são atribuídas a dados pessoais, dado que podem perfilar os utilizadores e estão nas mãos dos CSPs, logo, os fornecedores PaaS e IaaS que antes do RGPD, não tinham quase nenhum papel na proteção de dados, no âmbito do RGPD, recebem alguma responsabilidade (Russo, et al., 2018).

Karen Stendal (2020) afirma que, em caso de violação de dados pessoais, dado que os atacantes apagam a auditoria, e os dados forenses rastreiam os vestígios da sua intrusão, ocorre um problema de conformidade do RGPD, porque o CSP, enquanto processador, não consegue notificar o responsável sem atrasos indevidos, depois de ter tomado conhecimento de uma violação de dados pessoais. Consequentemente, a organização do cliente, enquanto controlador, não poderá notificar a violação de dados pessoais à autoridade de supervisão no prazo de 72 horas após ter tomado conhecimento do mesmo e sem demora injustificada. (Stendal, 2020).

6.1.2 Cliente em Nuvem como Controlador ou Processador

Se um fornecedor é um processador de dados, geralmente, um cliente de serviços na nuvem é considerado um controlador dos dados armazenados nos servidores do fornecedor. Como o caso de IaaS e PaaS, serviços em que o cliente determina como os dados são tratados e a finalidade para a qual são processados. O cliente é um processador se ela ou ele está apenas a processar os dados pessoais de acordo com os desejos de um terceiro como o caso do SaaS.

O RGPD atribui a responsabilidade por violações no tratamento de dados pessoais, como controlador de dados, mas adiciona uma responsabilidade partilhada com o processador, como controlador conjunto, quando o cliente não tem controlo direto dos dados e do seu processo (Russo, et al., 2018).

Karen Stendal (2020) concluiu que, embora as definições do controlador e do processador sejam as mesmas na Diretiva 95/46/CE e no RGPD, as suas responsabilidades mudaram no âmbito do RGPD. O controlador é definido da seguinte forma: a pessoa singular ou jurídica, a autoridade pública, a agência ou outro organismo que, sozinho ou em conjunto com outros, determine as finalidades e os meios de

tratamento dos dados pessoais; se os fins e meios dessa transformação forem determinados pela legislação da União ou dos Estados-Membros, o responsável pelo tratamento ou os critérios específicos para a sua nomeação podem ser previstos pela legislação da União ou dos Estados-Membros (Stendal, 2020).

6.1.3 Responsabilidades do Cliente e Fornecedor de Serviços na Nuvem como Controladores

No âmbito do RGPD, os clientes podem ter melhores meios para solicitar uma indemnização contra o prestador graças à introdução do controlo conjunto entre um prestador e os seus clientes, mantendo as duas funções distintas, agir como um processador estabeleceria de facto uma corresponsabilidade do prestador por quaisquer danos sofridos pelo indivíduo a quem os dados se referem. Tanto os fornecedores SaaS como os da IaaS partilham a responsabilidade dos dados pessoais tratados pelo que está dentro de cada competência. A responsabilidade conjunta, aplica-se a muitos serviços populares na nuvem (Russo, et al., 2018).

6.2 Políticas de Armazenamento e Processamento de Dados

Quando os CSPs oferecem serviços para armazenar persistentemente ou para elaborar dados sensíveis ou especiais para os serviços SaaS, o cumprimento do RGPD torna-se mais rigoroso, nomeadamente, quando oferecem esses serviços sob subcontratação. Assim, a prática da subcontratação na computação em nuvem estabelece uma cadeia de responsabilidades para a proteção de dados, que tem de ser rastreada e monitorizada (Russo, et al., 2018).

6.3 Consentimento dos Titulares dos Dados para Serviços na Nuvem

Implementar o consentimento dos titulares dos dados para serviços na nuvem pode ser um desafio, dado que nem sempre é claro onde os dados se encontram armazenados. É essencial, fornecer ao titular dos dados o contacto de uma pessoa responsável pela nuvem, para ser contactada em caso de violação. Os titulares dos dados têm o direito de reclamar por danos sofridos em resultado de uma violação do RGPD, mas a prova de consentimento recai frequentemente sobre o cliente dos serviços de nuvem como

responsável pelos dados, o qual, normalmente, não tem a competência técnica ou acesso para denunciá-lo.

Na prática, apenas o processador tem competência e conhecimento de como os dados recebidos através do controlador (como o SaaS) ou diretamente através das suas plataformas (como o IaaS e o PaaS) são efetivamente processados. Apenas o processador pode reter a prova dos consentimentos dos seus sujeitos e torná-la acessível às partes interessadas através das suas ferramentas de TI (Russo, et al., 2018).

6.4 Segurança e Violação de Dados

Os controladores e os processadores devem tomar medidas adequadas, tais como o pseudónimo e contramedidas, para evitar problemas de segurança como a perda de dados, a alteração de dados e o acesso não autorizado; tais medidas dependem da arquitetura em nuvem e da forma como processa os dados. Uma organização que permita aos colaboradores utilizar software pessoal em nuvem (como o Dropbox) dentro do IaaS da empresa pode estar diretamente exposta às consequências das violações do RGPD se o fornecedor iaaS não assumir qualquer responsabilidade ou medida. As violações de dados, como a divulgação não intencional de informações seguras ou privadas a uma parte não fidedigna, são uma das principais preocupações do RGPD; uma notificação detalhada da violação, incluindo a causa do incidente, deve ser comunicada o mais tardar 72 horas após a informação da organização (Russo, et al., 2018).

6.5 Localização e Transferência de Dados

Os dez melhores centros de dados do mundo estão localizados fora da Europa; os clientes e fornecedores, devem conhecer e monitorizar onde os dados são armazenados, dado que a localização física do centro de dados de um fornecedor, frequentemente, não corresponde à localização da sede do prestador. A localização de dados no RGPD também pode ter efeitos significativos nos serviços SaaS como o Microsoft Office 365, G Suite e Salesforce. Estas empresas são controladoras de dados no que respeita aos fornecedores, e processadores SaaS no que diz respeito a subscrição. Além disso, os fornecedores de SaaS como o G-Suite da Google têm de garantir que os seus subcontratantes localizados fora da UE, como os produtos *spanning* para proteção de dados, também aderem ao RGPD (Russo, et al., 2018). Crucialmente importante para a computação em nuvem, é

como transferir dados através das fronteiras da UE e quais as salvaguardas que devem ser implementadas para serem compatíveis com o RGPD; em 2017, os principais CSPs como IBM, Alibaba, Oracle e SAP assinaram um código de conduta compatível com o RGPD para os CSPs, enquanto grandes fornecedores de IaaS como Aruba, AWS e *UpCloud* assinaram um código de conduta específico compatível com o RGPD para os fornecedores IaaS.

6.6 Eliminação de Dados

O direito a ser esquecido, pode ser implementado de diferentes formas, dependendo do tipo de serviço na nuvem que processa os dados. Por exemplo, um fornecedor IaaS normalmente que não gere ou opte por apagar os dados dos clientes em seu nome, visto que o cliente é responsável por estas ações noutros casos, a forma de apagar dados é também uma questão técnica (Russo et al., 2018).

Computação na Nuvem — C Características	Está em conformidade?		RGPD - Artigos	Justificação
	Sim	Não		
Ambiente de nuvem virtual		X	Artigo 33.º (1, 2 e 3) - O processador notificará o responsável pelo tratamento sem demora injustificada sobre a violação de dados pessoais, o mais tardar 72h. Artigo 5.º, n.º 1-f — Integridade e Confidencialidade dos Dados	Os atacantes podem explorar vulnerabilidades no hipervisor e obter privilégios elevados, para aceder ao ambiente na nuvem e eliminar ou modificar os dados pessoais. Consequentemente, o responsável pelo tratamento não poderá notificar a violação de dados pessoais à autoridade de supervisão e fornecer detalhes sobre a violação no prazo de 72 horas.
Acordos contratuais simples e padrão da CSP		X	Artigo 28.º (1, 3-a e 4) — O processador deve garantir a proteção dos direitos do titular dos dados, informar o responsável pelo processamento acerca do requisito legal antes do processamento) Artigo 5.º (1-a) — legalidade, justiça e transparência.	Os CSPs e os seus subcontratantes tendem a fornecer acordos menos transparentes, sobre a complexidade do hardware de infraestrutura em nuvem e detalhes sobre a localização e tratamento de dados pessoais. Isso não está em conformidade com o RGPD ao fornecer garantias de proteção dos direitos dos titulares dos dados.
Backups distribuídos geograficamente		X	Artigo (7-2) — Consentimento - o pedido de consentimento deve ser apresentado de uma forma que é claramente. Artigo (17-1) — O titular dos dados tem o direito de obter do responsável pelo tratamento, o direito de eliminar os dados pessoais que lhe digam respeito, sem demora injustificada.	Não é claro onde estão as cópias de backup distribuídas dos dados pessoais, o que dificulta a obtenção do consentimento do titular dos dados de forma clara. Torna igualmente difícil garantir o direito ao apagamento, e garantir a eliminação de todas as cópias de cópias de segurança.
Modelos de Serviço		X	Artigo 20.º - Direito à portabilidade dos dados, Artigo (20-1) — O titular dos dados tem o direito de receber os dados pessoais que lhe digam respeito, Artigo 15 — Direito de acesso pelo titular dos dados, Artigo 16.º — Direito à retificação e Artigo 17.º - Direito de Eliminar ("direito a ser esquecido").	Portabilidade dos dados aumenta ao nível do IaaS e diminui ao nível de SaaS devido ao bloqueio do fornecedor. O papel dos CSPs passa de processador para controlador, quando o seu cliente é uma pessoa comum. Os CSPs ou as organizações dos clientes como controladores, podem não ter os seus mecanismos de portabilidade de dados integrados com métodos de acesso, retificação e apagamento.

Tabela 3 Resultado da Comparação entre Computação na Nuvem e RGPD, Fonte: (Stendal, 2020)

7. Conclusão

Com as informações recolhidas sobre a computação na nuvem, observa-se que esta tecnologia tem um papel bastante importante, na forma como as empresas de pequena dimensão sobrevivem face às empresas de grande dimensão, começando pelos inúmeros serviços disponibilizados. Mas o foco desta dissertação centra-se na segurança e privacidade, que são pontos que as empresas têm em comum e continuam a ser uma preocupação tanto para empresas como para os fornecedores da nuvem. Como os dados são acedidos pela Internet, a ameaça à integridade dos dados é maior, isto porque estes ficam mais expostos aos ataques dos *hackers* ou pessoas mal-intencionadas, logo, tanto o cliente como o fornecedor da nuvem, têm responsabilidade partilhada nesse campo, dependendo do tipo do serviço que as empresas contratam.

Para se lidar com o problema referente a segurança e privacidade de dados tanto no dia a dia como na nuvem, fez-se um estudo sobre a forma como os dados pessoais são tratados na UE e nos EUA. Notou-se que, apesar dos esforços dos norte-americanos, ainda há muito caminho a ser percorrido para igualar a Europa. Sabe-se que nos EUA a abordagem referente à privacidade dos dados é diferente, quando comparada com a UE. Na UE, há apenas uma entidade para regular a forma como os dados dos cidadãos europeus são tratados dentro ou fora da UE, enquanto que nos EUA cada Estado tem a sua entidade para lidar com a privacidade dos dados. Entretanto, existem pontos em comum, como, por exemplo, ambas as entidades defendem o direito dos titulares dos dados, apesar da definição ser substancialmente diferente.

A comparação feita entre RGPD e o CCPA, a respeito de quem é protegido e as informações a serem protegidas, leva-nos à conclusão de que ambas as entidades têm estes dois pontos em comum, mas com uma abordagem ligeiramente diferente uma da outra. Pode-se observar ainda que ambas se centram na informação relacionada com uma pessoa singular identificável, mas diferem nas definições. Ambas têm potenciais efeitos extraterritoriais que as empresas localizadas fora da jurisdição devem considerar; no entanto, a definição CCPA também inclui informações ligadas ao nível do agregado familiar.

Para estar em conformidade com as leis de privacidade, foram criadas novas responsabilidades para os fornecedores da nuvem, que é como processador ou controlador dos dados na nuvem. Anteriormente, SaaS era o único modelo de serviço para tratar e processar dados dos clientes; atualmente, foram criadas novas responsabilidades para o IaaS e o PaaS. O estudo elaborado revela que, apesar dos esforços dos fornecedores da nuvem, ainda falta muito caminho a ser percorrido em matéria de segurança e privacidade, começando pela parte em que os dados são acedidos pela Internet.

7.1 Trabalho Futuro

Como trabalho futuro, sugere-se acompanhar o processo de regulamentação brasileira no que toca à privacidade e proteção de dados pessoais e sensíveis, comparando com outras entidades como RGPD e o CCPA, para se poder perceber a maturidade da lei, a sua amplitude e a sua aplicação na nuvem. Seria também interessante comparar as três entidades, na forma como os dados pessoais são tratados na EU (RGPD), EUA (CCPA) e no Brasil (LGPD), visto que já obtivemos o resultado da comparação entre a EU e o EUA e também porque se apercebe que o Brasil deu início a este processo há pouco tempo, assim como os EUA.

7.2 Limitações

As limitações encontradas ao longo deste processo de investigação, foram a falta de documentação mais recente sobre a Diretiva Europeia de Proteção de Dados, bem como sobre as entidades que regulam e protegem os dados pessoais nos EUA para cada Estado, como, por exemplo, Nova Iorque, Carolina do Norte e outros Estados.

8. Bibliografia

AG, Horizon 2020 Framework Programme of the European Union and Proton Technologies. (28 de 06 de 2021). *what-is-gdpr*. (P. T. AG, Produtor, & Proton Technologies AG) Obtido em 28 de 06 de 2021, de GDPR.eu: https://gdpr.eu/what-is-gdpr/

Baker, J. A. (2019). The General Data Protection Regulation in the Age of Surveillance. *Journal of Business Ethics volume, 168*(3), 6-8. doi:https://doi.org/10.1007/s10551-019-04239-z

Barrett, C. (2019). (S. Lawyer, Ed.) *Are the EU, GDPR AND the California CCPA becoming the de Facto Global Standards for Data Privacy and Protection?, 15*(3).

Bussche, P. V. (2017). *The EU General Data Protection Regulation: A Practical Guide.* Berlin: Springer International Publishing AG.

Chorpash, J. (2020). Do You Accept These Cookies? How the General Data Protection Regulation Keeps Consumer Information Safe. (J. o. Business, Ed.) *40*(2), pp. 5-16.

Fachin, O. (2001). Fundamentos de metodologia. São Paulo: Saraiva.

Gazis, T. G. (2021). Humanitarian aid inthe age of COVID-19: A review of big data crisis analytics and the General Data Protection Regulation.

Goldman, P. E. (2020). An Introduction to the California Consumer Privacy Act (CCPA). *An Introduction to the California Consumer Privacy Act (CCPA)*, pp. 2-5.

Gupta, L. D. (2019). India's Personal Data Protection Act, 2018: Comparison with the General Data Protection Regulation and the California Consumer Privacy Act of 2018. *Berkeley Journal of International Law, 37*(3), 24-32.

Issa, N. G. (2021). Cloud Computing Security and Privacy Preservation: Using multi-level encryption. (M. University, Ed.) *The International Journal of Engineering and Information Technology, 7*(2). Obtido em 22 de July de 2021

Issi, H. N., & Ef, A. (2018). Cryptography Challenges of Cloud Computing For E-Government Services. *International Journal of Innovative Engineering Applications, 2*(1), 1-2.

Jehl, L., Friel, A., & LLP, B. (2018). CCPA and GDPR Comparison Chart. *A Chart comparing some of the key requirements of the California Consumer Privacy Act (CCPA) and the EU General Data Protection Regulation (GDPR).*, pp. 1-8.

Khan, B. D. (2020). The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities. *United States International Trade Commission*, pp. 4-5.

Khan, R., & Srivastava, P. (2018). A Review Paper on Cloud Computing. *International Journals of Advanced Research in Computer Science and Software Engineering*, *8*(6).

Laure, A. G. (2016). Security and Privacy of Sensitive Data in Cloud Computing: A Survey of Recent Developments. p. 8.

Lysobey, S. P. (2021). The California Consumer Privacy Act of 2018 Updated: More Protection in the Quest to Access and Protect Personal Information. *mcglinchey, 76*, 2-5.

Mammona, A. N., Kanwal, N., Fleury, M., Herbst, M., & Qiao, Y. (2019). Visual Surveillance Within the EU General Data Protection Regulation: A Technology Perspective.

Microsoft. (22 de July de 2021). *Microsoft*. (Micorsoft Corporate) Obtido em 22 de July de 2021, de Microsoft Azure : https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/

Moerel, L. (2011). The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide? 5-7.

Okoli, C., (2015) "A Guide to Conducting a Standalone Systematic Literature Review" *Communications of the Association for Information Systems*, Vpl. 37, Article 4

Peasley, M. (2019). It's Time For an American (Data Protection) Revolution. *Akron Law Review, 52*(3), 7-20, 28-29.

Russo, B., Valle, L., Bonzagni, G., Locatello, D., Pancaldi, M., & Tosi, D. (2018). Cloud Computing and the New EU General Data New EU General Data. *IEEE Computing Society*, 3-7.

Salehi, A. W., Noori, F., & Saboori, R. (2019). Cloud Computing Security Challenges and its Potential Solution. *American Journal of Engineering Research, 8*(10).

Simmon, E. (2018). Evaluation of Cloud Computing Services Based on NIST SP 800-145. p. 8.

Simmons, M. R. (2021). New Virginia Privacy Law Promises Big Impacts. *The Computer & Internet Lawyer, 38*(6).

Stendal, R. E.-G. (2020). Examining How Gdpr Challenges Emerging Technologies. *Journal of Information Policy, 10*, 14-17.

Taghipour, M., Mowloodi, E. S., Mahboobi, M., & Abdi, J. (2020). Application of Cloud Computing in System Management in Order to Control the Process. *3*(3), pp. 3-4.

Ventura, L. (2020). “Senator, We Run Ads”: Advocating for a US Self-Regulatory Response to the EU General Data Protection Regulation. (S. C. Ondrof, Ed.) *28*(2).

Voss, G. W., & Houser, K. A. (2019). Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies. p. 9.

Wulandari, R., Jonas, D., & Alwarits, N. F. (2020). Design Of Expert System Application for Android Based DSLR Camera Damage Diagnostics. (U. o. Raharja, Ed.) *IAIC Transactions on Sustainable Digital Innovation, 1*(2).